Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Informatica per il management

ANALISI, PROBLEMATICHE E SOLUZIONI RELATIVE AI RISCHI CONNESSI AI DATI AZIENDALI

Relatore:
Chiar.mo Prof.
Edoardo Mollona

Presentata da:
Alberto Donati

Sessione III
Anno Accademico 2018/2019

Indice

Introduzione

Nel corso degli anni si è potuto vedere quanto i dati siano importanti per le aziende. I dati possono creare enormi guadagni (o danni) sia alle aziende medio/piccole sia alle grandi multinazionali. Non sempre le aziende si rendono conto di quanto i dati siano fondamentali per continuare a lavorare. Questa tesi vuole fare un'analisi della gestione dei dati e dei rischi ad essi connessi. Propone inoltre delle soluzioni su come prevenire i danni ai dati e un caso di un'azienda che è riuscita a non fallire nonostante un grave incendio che ha distrutto la sede.
Il primo capitolo illustra approfonditamente i rischi a cui possono andare incontro i dati aziendali. In questo capitolo vengono descritti diversi tipi di rischio legati ai dati, alcuni più comuni che altri.
Nel secondo capitolo vengono esposti alcuni articoli e motivi del Regolamento Europeo 2016/679, chiamato anche GDPR.
Nel terzo capitolo viene spiegato cos'è e cosa contiene il piano di Disaster Recovery. Questo piano viene spesso sottovalutato dalle aziende perché pensano che incidenti gravi non capiteranno mai proprio a loro.
Il quarto capitolo descrive la situazione attuale delle Pubbliche Amministrazioni. Inoltre, mostra la situazione attuale delle aziende.
Nel quinto capitolo viene illustrato il caso di Bitways S.r.l., un'azienda che è andata distrutta in un incendio il 9 agosto 2019 e comunque è riuscita a ripartire. Questa azienda è riuscita a tornare a lavorare e successivamente ha creato e portato avanti una campagna crowdfunding ottenendo dai sostenitori più di 30000 euro.
Nel sesto capitolo vengono viste le principali configurazioni RAID, queste vengono usate per consentire la ridondanza dei dati e/o la loro rapida accessibilità. Queste vengono quindi adottate per evitare la perdita di dati in caso di rottura di dischi.

Nel settimo capitolo vengono spiegate alcune delle principali tipologie di backup attualmente utilizzate.
Infine, nell'ottavo capitolo vengono mostrate diverse tipologie di servizi cloud e l'importanza per un'azienda di affidarsi sia per motivi logistici sia per motivi economici a servizi cloud.

Capitolo 1

Rischio

1.1 Risk management

Il risk management, detto anche analisi del rischio, è l'insieme di attività, metodologie e risorse coordinate per guidare e tenere sotto controllo un'organizzazione con riferimento ai rischi.

Il risk management viene diviso in identificazione, analisi e valutazione, nello Standard BS ISO 31000:2018

> *"Risk assessment is the overall process of risk identification, risk analysis and risk evaluation".*

Nell'identificazione del rischio vengono considerati diversi fattori (rif. Standard BS ISO 31000:2018)

- fonti di rischio tangibili e intangibili
- cause ed eventi
- minacce ed opportunità
- vulnerabilità e capacità
- cambiamenti nel contesto esterno ed interno

- indicatori di rischi emergenti
- la natura e il valore dei beni e delle risorse
- conseguenze e il loro impatto sugli obiettivi
- limitazione della conoscenza e affidabilità dell'informazione
- fattori relativi al tempo
- pregiudizi, presupposti e convinzioni delle persone coinvolte

La valutazione del rischio considera i fattori come (rif. Standard BS ISO 31000:2018)

- la probabilità degli eventi e conseguenze
- la natura e la grandezza delle conseguenze
- complessità e connessione;
- fattori relativi al tempo e volatilità
- l'efficacia dei controlli esistenti
- livelli di sensibilità e fiducia

A seguito della identificazione e analisi del rischio, la valutazione può portare a decisioni come (rif. Standard BS ISO 31000:2018)

- non fare altro
- considerare le opzioni di trattamento del rischio
- svolgere ulteriori analisi per comprendere meglio il rischio
- mantenere i controlli attuali
- riconsiderare gli obbiettivi

1.2 I rischi nell'IT

Ci possono essere molti tipi di rischio all'interno dell'azienda, che vanno attentamente valutati e non sottovalutati. In questa parte vengono descritti i possibili tipi di rischio a cui possono venire incontro le infrastrutture e i dati.

Definiamo 3 categorie

- eventi riconducibili al comportamento umano
- riconducibili agli strumenti informatici
- eventi riconducibili al contesto fisico-ambientale

1.3 Eventi riconducili al comportamento umano

1.3.1 Sostituzione di persona

Un soggetto esterno o interno alla società potrebbe accedere ai dati aziendali con le credenziali del legittimo proprietario, sostituendosi interamente al titolare delle stesse.
Il seguente caso può avvenire ad esempio per

- distrazione del dipendente che lascia incustodita la propria postazione di lavoro
- scambio di credenziali tra dipendenti
- negligenza nel lasciare in posti non sicuri le credenziali
- problematiche nel sistema di gestione delle autenticazioni

1.3.2 Distrazione / negligenza

Possono essere di tipo "fisico" o "logico".
La distrazione/negligenza di tipo "fisico" comporta danni fisici agli strumenti di lavoro e potrebbe causare anche danni ai dati.
La distrazione/negligenza di tipo "logico" invece determina solamente un danneggiamento ai dati. Ad esempio un lavoratore distratto potrebbe non salvare correttamente un file.

Altri esempi sono cancellare file ed eseguire comandi non voluti che provocano la perdita di dati.

1.3.3 Atto doloso

È il rischio più grave e pericoloso perché c'è una diretta volontà nel creare problematiche, manomettere strumentazioni o distruggere dati.

1.4 Eventi riconducibili agli strumenti informatici

1.4.1 Virus informatico

Esistono dei virus appositamente creati per cancellare o danneggiare i dati o per causare l'interruzione del lavoro aziendale. Negli ultimi anni sono stati creati dei virus particolari che vanno a criptare i dati aziendali. Per cui i file rimangono integri e presenti sul PC della "vittima" ma non sono utilizzabili. La soluzione proposta dai criminali informatici attori dell'attacco è invitare la "vittima" al pagamento di un "riscatto" per riavere i dati come prima. L'azione dei virus informatici potrebbe avvenire tramite download da siti non sicuri, download e apertura di allegati provenienti da mail o macro dannose presenti in documenti.

1.4.2 Malfunzionamento delle strumentazioni aziendali

Le strumentazioni informatiche possono essere soggette a rotture o malfunzionamenti dati dalla macchina stessa. Una macchina potrebbe essere obsoleta e rompersi inavvertitamente. A seconda del guasto si può avere un'interruzione delle attività lavorative o potrebbe anche portare alla perdita di dati.

1.4.3 Malfunzionamento software

Ci possono essere difetti nel software utilizzato dall'azienda che al momento dell'acquisto non erano facilmente identificabili o non erano presenti. Ogni programma dipende da altro software e hardware presente nella macchina. Un esempio di problematica è la

corruzione dei file di sistema. I problemi software possono portare ad una indisponibilità temporanea dei servizi e dei dati aziendali necessari per l'attività lavorativa.

1.4.4 Accesso esterno non autorizzato

Intrusioni e accessi non autorizzati mediante attacco informatico diretto via internet, senza furto di credenziali. Questi avvengono sfruttando vulnerabilità del sistema informatico.

1.5 Eventi riconducibili al contesto fisico-ambientale

1.5.1 Ingresso non autorizzato a locali ad accesso riservato

Esiste la concreta possibilità che soggetti non autorizzati entrino fisicamente all'interno dei locali aziendali in cui sono presenti le infrastrutture e strumentazioni informatiche. Si possono verificare quindi gravi perdite di dati causati dalla modifica o dalla distruzione delle infrastrutture e strumentazioni.

1.5.2 Sottrazione/furto di strumenti contenenti dati personali

È possibile che venga sottratto un PC o uno storage contente i dati aziendali. Nel caso questi dati non fossero presenti su altri strumenti di archiviazione (anche su internet) c'è la perdita di tutti i dati.

1.5.3 Guasto elettrico/internet

I sistemi elettrici e le connessioni internet potrebbero venire a meno. Questo non a causa dell'azienda ma del provider fornitore del servizio. I provider potrebbero essere andati incontro a dei guasti sulle linee. Questi guasti potrebbero provocare dei disservizi lavorativi anche gravi.

1.5.4 Eventi distruttivi naturali o artificiali

(rif. anche a Snedaker, S 2013, Business Continuity and Disaster Recovery Planning for IT Professional ; Wallace, M, & Webber, L 2004, Disaster Recovery Handbook)

Si considerano gli eventi di diversa natura che provocano distruzione parziale o totale di infrastrutture e strumentazioni informatiche. Questo potrebbe portare ad una indisponibilità prolungata di dati e servizi. Nei casi più gravi anche la perdita parziale o totale dei dati.

Incendio

Gli incendi sono una delle cause più comuni di disastro con cui le aziende hanno a che fare. Gli incendi oltre a causare vittime e feriti causano anche la distruzione delle infrastrutture e degli edifici. È importante capire cosa si possa fare in caso di incendio per rispondere prontamente alle emergenze. Potrebbe essere utile contattare i propri assicuratori per capire come adottare le misure necessarie per prevenire gli incendi. I corsi per saper usare gli estintori e gestire le emergenze dell'incendio sono un buon modo per poter poi gestire correttamente un incendio.

Allagamento

Gli allagamenti derivano da grandi quantità d'acqua che entrano negli ambienti lavorativi o dall'interno o dall'esterno dell'edificio. Possono, ad esempio, essere causati da

- Inverni rigidi o estati piovose
- Nevicate abbondanti
- Straripamento di fiumi
- Tempeste tropicali
- Tsunami (che potrebbero causare inondazioni)

Fulmine

I fulmini possono presentarsi in qualsiasi stagione e clima. I fulmini possono causare sbalzi di corrente, incendi, danneggiare gli edifici e ferire od uccidere persone e animali. Per risolvere gli sbalzi di tensione diverse aziende si dotano di UPS. Questi UPS vanno opportunamente testati e controllati per garantire la continuità lavorativa in caso di problemi.

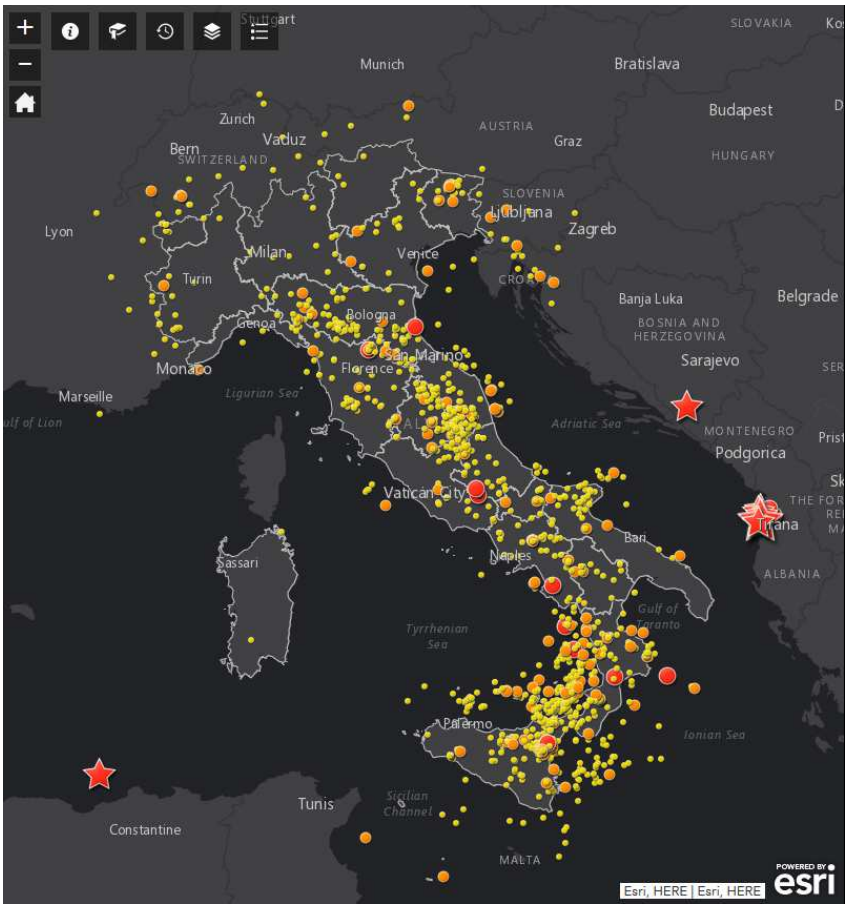
Siccità

Anche se comunemente non viene considerato un problema, invece potrebbe causare danni economici non indifferenti. Secondo il National Drought Mitigation Center della University of Nebraska in Lincoln (UNL)

> *"Drought produces a complex web of impacts that spans many sectors of the economy and reaches well beyond the area experiencing physical drought. This complexity exists because water is integral to our ability to produce goods and provide services. Impacts are commonly referred to as direct or indirect. Reduced crop, rangeland, and forest productivity; increased fire hazard; reduced water levels; increased livestock and wildlife mortality rates; and damage to wildlife and fish habitat are a few examples of direct impacts" (National Drought Mitigation Center, 2013).*

Terremoto

I terremoti sono un evento che si verifica anche in Italia. I terremoti potrebbero causare grandi rallentamenti alle comunicazioni oltre che alla distruzione di edifici. I rallentamenti alle comunicazioni porterebbero problemi non indifferenti in un'azienda che si occupa di IT. I terremoti, nella zona italiana, con magnitudo superiore o uguale a 2.0 sono stati 1848, la magnitudo massima raggiunta è stata di 6,2.



Fonte: INGV

Tornado

Un tornado è una colonna d' aria che si verifica sulla terra (a differenza degli uragani che si originano sull'acqua). I danni dei tornado sono solitamente limitati alla zona in cui avviene, ma spesso sono imprevedibili. Come le persone che vivono in zone con possibili terremoti, anche le persone che vivono in zone in cui si verificano i tornado hanno delle precauzioni. I tornado, oltre ad avere un impatto sugli edifici delle aziende, hanno un impatto molto forte sui dipendenti. Ad esempio, nel caso venisse distrutta la l'abitazione di familiari, amici o vicini.

Uragano

Uragano secondo Treccani.it

> *"Denominazione del ciclone tropicale usata comunem. nelle Indie Occidentali, negli Stati Uniti merid. e in Australia: è caratterizzato da una depressione molto profonda il cui forte gradiente di pressione genera venti impetuosi con andamento a spirale, che cominciano a turbinare verso l'alto quando raggiungono il nucleo della perturbazione dando origine a una struttura di cumulonembi disposta intorno all'occhio del ciclone (il cosiddetto «muro dell'occhio»)".*

Gli uragani sono anche essi molto pericolosi e devastanti sia per le abitazioni, sia per le aziende, sia per le persone. Gli uragani hanno origina sopra l'acqua ma possono viaggiare attraverso la terraferma e causare enormi danni nelle zone costiere e non.

Tsunami

Gli tsunami sono delle grandi onde generate da terremoti, eruzioni vulcaniche o grandi frane. È importante capire il potenziale rischio degli tsunami e adottare le giuste strategie per fare in modo che gli tsunami creino meno danni possibili.

Vulcano

I vulcani sono fratture della superficie terrestre attraverso cui escono il magma e diversi gas associati. La forma del vulcano è data dal materiale eruttato e hanno tipicamente una forma conica. I vulcani, come altre calamità naturali, possono verificarsi senza preavviso. A differenza però di altri pericoli, i punti sono ben noti. Le imprese delle aree vulcaniche dovrebbero preparare piani di evacuazione adeguati in modo da essere preparate all'eventualità che l'edificio venga inondato dalla lava.

Neve

Le forti nevicate o bufere di neve possono chiudere le strade di accesso che portano all'interno e all'esterno dell'edificio. Questo potrebbe obbligare i dipendenti a rimanere a casa. Le tempeste di neve vanno monitorate per capire quando è possibile riprendere le attività lavorative. Della neve ammucchiata sopra gli edifici potrebbe portare a problemi strutturali, che porterebbero anche a danni economici. L' opzione di accedere ai dati

aziendali da remoto può essere una buona soluzione per continuare a lavorare da casa fintanto che non è possibile rientrare negli ambienti lavorativi.

Temperatura estrema

Temperature molto calde o molto fredde, possono danneggiare le strutture aziendali e i materiali. Inoltre, potrebbero creare delle condizioni non favorevoli all'ambiente lavorativo. È utile dotarsi quindi di buoni impianti di condizionamento nel caso le temperature esterne siano molto calde o molto fredde. Gli impianti di condizionamento hanno un costo di energia che si traduce in un costo economico.

Emergenza sanitaria

Le emergenze sanitarie possono provocare gravi problemi economici dati ad esempio dallo sfollamento dalle città, dagli stop produttivi, dal contagio. Attualmente è noto il caso del nuovo coronavirus SARS-CoV-2, come descritto dal portale dell'epidemiologia per la sanità pubblica a cura dell'ISS

> *"Il 31 dicembre 2019, le autorità sanitarie cinesi hanno notificato un focolaio di casi di polmonite ad eziologia non nota nella città di Wuhan (Provincia dell'Hubei, Cina). Molti dei casi iniziali hanno riferito un'esposizione al Wuhan's South China Seafood City market (si sospettava un possibile meccanismo di trasmissione da animali vivi). Il 9 gennaio 2020, il China CDC (il Centro per il controllo e la prevenzione delle malattie della Cina) ha identificato un nuovo coronavirus (provvisoriamente chiamato 2019-nCoV) come causa eziologica di queste patologie. Le autorità sanitarie cinesi hanno inoltre confermato la trasmissione inter-umana del virus. L'11 febbraio, l'Organizzazione Mondiale della Sanità (OMS) ha annunciato che la malattia respiratoria causata dal 2019-nCoV è stata chiamata COVID-19 (Corona Virus Disease).*
>
> *Il Gruppo di Studio sul Coronavirus (CSG) del Comitato internazionale per la tassonomia dei virus (International Committee on Taxonomy of Viruses) ha classificato ufficialmente con il nome di SARS-CoV-2 il virus provvisoriamente chiamato dalle autorità sanitarie internazionali 2019-nCoV e responsabile dei casi di COVID-19 (Corona Virus Disease)".*

Terrorismo / violenza

Il terrorismo è un fenomeno difficilmente prevedibile. Anche se non interessa solitamente le aziende, comunque potrebbe interessare un posto vicino. Violenza all'interno o nell'area vicina all'azienda, specialmente riguardo conflitti tra dipendenti, portano ad avere giudizi negativi verso l'azienda. Episodi di terrorismo o violenza tenderanno a creare un'immagine non positiva dell'area in cui è presente l'azienda.

Capitolo 2

GDPR

2.1 Cos'è

Il Regolamento Europeo 2016/679 (GDPR) è la regolamentazione europea in cui viene descritta dettagliatamente la disciplina della privacy maturata negli anni in Europa. Questo regolamento ha lo scopo di raccogliere in un documento la privacy e rendere unitaria la materia.

2.2 Articolo 32 - Sicurezza del trattamento

L'articolo 32 non è esaustivo sulle misure di sicurezza da adottare. Non è quindi possibile stabilire in alcun modo se le misure adottate siano necessarie o sufficienti. Spetta quindi al titolare e al responsabile del trattamento stabilire quali misure adottare in base al rischio.

> *1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

2.3 Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

L'articolo 33 descrive cosa bisogna fare in caso di violazione dei dati personali e come eseguire la segnalazione all'autorità di controllo competente nel caso fosse necessaria.

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i

provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

2.4 Motivo 74

Il motivo 74 descrive la responsabilità generale del titolare del trattamento.

È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

2.5 Motivo 75

Il motivo 75 descrive i rischi legati alle persone derivati dal trattamento di dati personali.

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla

vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

2.6 Motivo 83

Il motivo 83 descrivono il rischio legato ai dati e i fattori da tenere in considerazione che potrebbero causare un qualsiasi tipo di danno.

Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Capitolo 3

Disaster Recovery

3.1 Cos'è il Disaster Recovery e il piano di Disaster Recovery

Il Disaster Recovery è la capacità di ripristinare in maniera ottimale i dati e l'operatività di un azienda dopo un disastro di qualsiasi tipo.

Il Disaster Recovery è uno scenario estremo che può illustrare molto bene l'utilità del cloud. Per molte aziende, prepararsi alla perdita dei propri dati o alla possibilità di non essere più connessi ad internet è una perdita in termini di tempo e/o costo. Le aziende piccole e medie non percepiscono né il valore del Disaster Recovery né il rischio legato alle infrastrutture IT. Queste aziende sono quindi scoperte nei confronti di qualunque grande crisi informatica.
Il piano di Disaster Recovery ha la funzione di descrivere in maniera dettagliata le fasi necessarie per il ripristino dei dati e delle funzionalità aziendali.
Il piano di Disaster Recovery permette di stabilire le corrette procedure da seguire in caso di disastro per garantire il rapido ripristino dell'azienda. Attraverso dei test periodici l'azienda controlla che le procedure di Disaster Recovery siano ottimali e verifica che i backup siano svolti correttamente.

3.2 Business continuity

La business continuity o continuità operativa è la continuità del business, cioè la capacità di essere sempre operativi. La business continuity è solitamente gestita da un Responsabile. In aziende molto grandi potrebbe esserci anche un comitato apposito per la gestione della business continuity.
La business continuity è molto importante per un azienda, specialmente per un azienda che tratta di IT. Le aziende hanno bisogno di andare avanti e cercare di perdere meno dati e meno tempo possibile per il ripristino delle normali funzionalità dell'azienda.

La business continuity viene garantita dall'esecuzione di diversi stage, questi stage vengono definiti nello Standard BS ISO/IEC 24762:2008

> *" a) Establishing business recovery priorities, timescales and requirements (including first conducting business impact analysis review and risk assessment);*
> *b) Business continuity strategy formulation;*
> *c) Business continuity plan production;*
> *d) Business continuity plan testing;*
> *e) Ensuring business continuity awareness for all staff;*
> *f) Ongoing business continuity plan maintenance;*
> *g) Risk reduction."*

I piani di business continuity vanno periodicamente revisionati ed aggiornati, come descritto nello Standard BS ISO/IEC 24762:2008

> *"All policies, plans and provisions made should be documented. Staff at the relevant levels should be assigned to ensure that each document is reviewed and updated periodically. A configuration management system should be used to maintain current versions of documents, as well as of such as software and asset inventories".*

3.3 Comitato di Gestione Crisi

Viene nominato e poi successivamente scritto nel piano di Disaster Recovery un Comitato di Gestione Crisi. Questo Comitato è al vertice nella gestione del disastro e spetta ad esso prendere le principali decisioni al riguardo.

Il Comitato di Gestione Crisi si occupa di

- Valutazione dello stato di emergenza
- Decisione di far partire il piano di Disaster Recovery e controllo delle attività di recupero
- Comunicazione con esterni e dipendenti del disastro
- Redazione del report di fine emergenza
- Revisione del piano di Disaster Recovery

3.4 Responsabile del piano di Disaster Recovery

Al vertice del Comitato di Gestione Crisi c'è il Responsabile del piano di Disaster Recovery che:

- Provvedere a contattare tutte le figure che fanno parte del comitato di Gestione Crisi
- Provvede a aggiornare insieme al Comitato di Gestione Crisi il piano di Disaster Recovery
- Verifica l'aggiornamento del piano di Disaster Recovery
- Verifica i test e le esercitazioni riguardanti il piano di Disaster Recovery

3.5 Quando si decide di attivare il Comitato

Il Comitato viene attivato a discrezione del Responsabile, dopo aver valutato attentamente il problema.
Se prendiamo il piano di Disaster Recovery eseguendo per intero la procedura di Disaster Recovery completa, significa ripartire da zero con l'azienda eccetto ciò che si è salvato dal disastro. Ad esempio, dover comprare nuovi i server e i computer e riscaricare per intero i dati e gli applicativi.
Nel caso non sia necessario attivarlo, possono comunque esserci degli altri casi in cui bisogna intervenire seguendo una procedura decisa in precedenza, Si andranno quindi a creare delle procedure, in parti simili ma meno "radicali" del piano di Disaster Recovery. Esempi possono essere l'indisponibilità della sede per eventi atmosferici o terremoti oppure la mancanza di energia elettrica o della connettività internet.

3.6 Rischi considerati dal piano di Disaster Recovery

La procedura di Disaster Recovery considera, ad esempio, i rischi legati all'indisponibilità prolungata di internet, all'indisponibilità prolungata della rete elettrica, alla distruzione delle infrastrutture IT e all'impossibilità di accedere agli uffici.

3.7 Fasi del piano di Disaster Recovery

Di seguito le principali fasi della procedura di Disaster Recovery completa.

1. Valutazione della crisi/disastro/problema agli uffici lavoratiti
2. Dichiarazione di disastro da parte del Responsabile di Disaster Recovery
3. Comunicazione al Comitato di Gestione Crisi delle problematiche
4. Attivazione del personale responsabile delle fasi della procedura
5. Attuazione fasi della procedura
6. Dichiarazione di fine emergenza e redazione report

3.8 Cos'è il RTO

RTO significa Recovery Time Objective, rappresenta il tempo massimo accettabile per l'azienda per il ripristino della operatività aziendale. Il RTO viene infatti definito nello Standard BS ISO/IEC 27031:2011 come:

> *"recovery time objective*
> *RTO*
> *period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions must be recovered after a disruption has occurred".*

3.9 Cos'è il RPO

RPO significa Recovery Point Objective, rappresenta la perdita massima di dati tol-lerata dall'azienda. È il valore che descrive il periodo di tempo che trascorre tra il momento in cui il dato viene prodotto e la sua archiviazione in sicurezza tramite opportune procedure di backup.

Il RPO viene infatti definito nello Standard BS ISO/IEC 27031:2011 come:

> *"recovery point objective*
> *RPO*
> *point in time to which data must be recovered after a disruption has occurred".*

Fonte: elaborazione dell'autore

3.10 Test di ripristino totale

Ci sono dei test di ripristino totale dei dati che sarebbe meglio eseguire almeno ogni 6 o 12 mesi. Anche se i backup sono andati a buon fine, non è detto che si riesca a recuperare tutto, ma ci potrebbero essere alcuni problemi. Alcuni dei problemi potrebbero essere l'inconsistenza dei dati, la corruzione dei dati ecc.

3.11 Quando aggiornare il piano di Disaster Recovery

Il piano di Disaster Recovery verrà aggiornato periodicamente ogni tot anni e inoltre verrà modificato anche quando si andrà ad utilizzare. L'aggiornamento include gli eventuali allegati. Il piano o i suoi allegati verranno potrebbero dover essere aggiornati per eventi come:

- Acquisto di nuove apparecchiature informatiche
- Modifiche del personale facente parte del Comitato di Gestione Crisi
- Modifiche dei fornitori di servizi internet
- Modifiche dei fornitori di energia elettrica
- Modifiche dei fornitori di hardware
- Modifiche dei fornitori di software

3.12 Statistiche sulle conseguenze provocate dalla perdita di dati

- Oltre il 70% delle aziende coinvolte in un grave incendio non riapre o fallisce entro 3 anni dall'incendio. (rif. https://www.chubb.com/csc/chubb5836.html (2008))
- L' 80% delle aziende che hanno avuto un grave incidente non riaprirà mai o chiude entro 18 mesi. (rif. Source, Axa)

- L' 80% delle aziende che hanno sofferto di un disastro ai computer, che non hanno procedure di Disaster Recovery, falliscono. (rif. IBM Business Recovery Service & Cranfield (1993) A Bridge Too Far)
- Il 90% delle compagnie che hanno avuto perdite di dati falliscono entro 2 anni. (rif. http://www.nbnnews.com/ (2005))
- Le compagnie che non riescono a riprendere le operazioni entro 10 giorni da un disastro probabilmente non sopravvivranno. (rif. www.pctracker.info)
- La percentuale di compagnie che sopravvivono senza un piano di Disaster Recovery è meno del 10%. (rif. iosafe.com , www.hoc.co.uk , www.telcheck.co.uk)
- Il 43% delle compagnie a cui capitano incendi, alluvioni, mancanza di corrente, terrorismo, disastro software o hardware che non hanno un piano di Disaster Recovery non riapriranno mai. (rif. Cincinnati Business Courier (2004) Without a disaster recovery plan, your business is at risk, https://www.bizjournals.com/cincinnati/stories/2004/08/09/focus5.html)

Capitolo 4

Situazione attuale

4.1 Situazione Pubbliche Amministrazioni

Le pubbliche amministrazioni sono negli ultimi tempi attaccate da minacce informatiche. Le pubbliche amministrazioni hanno lo "svantaggio" di possedere e dover gestire milioni di informazioni.
Ad oggi i dati sanitari protetti sono informazioni la cui violazione è regolata da leggi nazionali e internazionali. Una delle principali cause di violazione è l'errore umano, che è un fenomeno globale e non localizzato. Con il passare del tempo i virus di tipologia ransomware si sono evoluti molto.
Ad esempio, in Italia si sono presentati attacchi come quello del 2016, riguardo le mail aziendali dell'ASP Basilicata. Sul sito ASP Basilicata si può infatti leggere

> *"L'ultima minaccia rilevata consiste in un potente Malware, battezzato con il nome di JS /TrojanDownloader.Nemucod, che si diffonde attraverso email scritte "in modo molto affidabile" che appaiono come fatture, atti giudiziari o altri documenti ufficiali. Le mail contengono un allegato malevolo che, se aperto, scarica e installa il malware sul computer delle vittime".*

Nel 2017 venne il famoso ransomware WannaCry, che creò non pochi problemi alle strutture ospedaliere

> *"in Gran Bretagna è allarme dopo che il malware ha infiltrato i sistemi di diversi ospedali. Le strutture, in tilt informatico, stanno invitando a chiunque*

non sia gravemente ferito a non recarsi nei pronto soccorso, impossibilitati all'accettazione. Dirottate le ambulanze." (Repubblica.it)

Nel marzo 2018 l'ASST della Valcamonica ebbe un grave guasto tecnico, per cui riuscirono a garantire solamente le Emergenze, le Urgenze e le attività rivolte ai pazienti degenti. La Gazzetta delle Valli riporta infatti la comunicazione dell'ASST

> *"purtroppo, dopo aver provveduto a quanto necessario per far ripartire il sistema questo non ha risposto, causando anzi un nuovo completo blocco degli apparati".*

Nell'aprile delle stesso anno si è stato registrato un attacco ad un Comune, quello di Bologna

> *"si è registrato un attacco informatico alla rete civica Iperbole, il sito web del Comune di Bologna: lo rende noto Palazzo d'Accursio. E ancora oggi il sito di Palazzo d'Accuriso non è accessibile, perchè "in manutenzione". L'attacco, a opera di Anonplus, "si è manifestato con la modifica di alcuni contenuti presenti nel sito, fra cui la home page", ed è ancora in corso, "in quanto, nonostante si sia provveduto al ripristino dei contenuti, questi sono stati modificati nuovamente"".(Repubblica.it)*

Ci sono stati problemi anche in molti comuni del mondo nel 2019, nelle PA il blocco dei servizi non comporta solamente una perdita finanziaria come nelle aziende ma anche il blocco di servizi utili ai cittadini e alle imprese.

> *"Il 2019 è stato l'anno degli attacchi ransomware rivolti ai Comuni. Durante gli ultimi 12 mesi, infatti, sono state prese di mira nel mondo almeno 174 istituzioni comunali e oltre 3.000 organizzazioni collegate, con un aumento del 60% rispetto al 2018. Mentre le richieste di riscatto dei criminali informatici raggiungono talvolta fino a 5 milioni di dollari. Sono alcuni dei dati contenuti nel Rapporto di Kaspersky Security Bulletin: Story of the Year 2019"(ANSA).*

Diversi problemi nelle PA sono causati, oltre dalla disattenzione del personale, dall'obsolescenza di alcuni macchinari. Questi macchinari obsoleti rendono il sistema più vulnerabile quando vengono connessi in rete.

AgendaDigitale.eu (il più grande network in Italia di testate e portali B2B dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale) tende a considerare l'età del personale come causa di problemi nelle PA

> *"Nelle PA e in particolare nei Comuni, l'età media dei dipendenti è di 51 anni e la classe che registra la maggiore concentrazione di lavoratori, pari al 24,9%, è quella dei 55-59enni. Il blocco del turnover ha precluso l'ingresso di personale giovane e ha determinato nel contempo l'esigenza di allungare la vita lavorativa per sostenere i sistemi previdenziali, rallentando il processo di rinnovamento del personale. La prossimità del personale all'età pensionabile, inoltre, ha inciso notevolmente sulla predisposizione alla formazione. Le debolezze da fattore umano e il quadro dell'infrastrutture sono le precondizioni affinché un attacco ransomware diventi devastante".*

Secondo un rapporto Verizon del 2018 le intrusioni nel settore sanitario sono aumentate dal 17% al 24 % in un anno, tra le debolezze principali il fattore umano: il 56% degli incidenti è causato da lavoratori interni.

Rimane inoltre il problema del phishing, il phishing viene definito dal Commissariato di Polizia Postale come

> *"È una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli".*

Agenda Digitale scrive al riguardo

> *"il phishing rappresenta il 98% degli attacchi messi a segno per estorcere denaro e il 93% di tutte le violazioni su cui il report ha indagato. L'anello debole continuano ad essere le e-mail. Se, infatti, nella media generale di tutti i settori considerati nel rapporto, i data breach sono causati nel 73% dei casi da attori "esterni" alla organizzazione e solo nel 28% dei casi da "interni", nell'healthcare la percentuale si inverte: il 56% degli incidenti è causato da attori interni, e solo il 43% da esterni. Nel maggior numero dei casi, questi "interni" contribuiscono all'incidente di sicurezza sotto forma di misdelivery (62%) ovvero invio di dati a destinatari errati, seguito da misplacing assets,*

misconfigurations, and disposal errors, ovvero da errori nella gestione appropriata dei dispositivi informatici. Secondo il Rapporto, nell'healthcare la probabilità di incidenti di sicurezza dovuti a queste diverse tipologie di errore è quasi sette volte maggiore di quella presente negli altri settori industriali".

4.1.1 Cosa è stato fatto per le Pubbliche Amministrazioni

Per la gestione dei dati da parte della PA è presente il Decreto Legislativo 7 marzo 2005, n.82, Codice dell'amministrazione digitale, nominato anche CAD.

In questo Decreto era presente un articolo molto importante, il 50-bis, questo articolo è stato abrogato con l'articolo 64 del Decreto Legislativo 26 agosto 2016, n. 179.

Il 50-bis disponeva che le PA dovessero adottare un piano di continuità operativa ed un piano di Disaster Recovery. Il piano teneva in considerazione anche le problematiche riscontrabili e gli aggiornamenti di esso.

Il Consiglio di Stato ha precisato che la disciplina dettata dall'abrogato 50-bis fosse inclusa nell'articolo 51 del CAD

"nella parte in cui dispone che le regole tecniche di cui all'art. 71 del CAD debbano anche individuare delle modalità che garantiscano l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture informatiche, in attuazione, peraltro, del criterio di delega di cui all'art. 1. comma 1, lett. m) della Legge n. 124 del 2015 (Consiglio di Stato, Commissione Speciale, 17 maggio 2016, parere n. 1024/2016)".

Per cui sono state rese più flessibili le indicazioni riguardo la continuità operativa e il Disaster Recovery, avendo tenuto conto anche delle tecnologie in rapida evoluzione.

Le pubbliche amministrazioni secondo l'articolo 17 del CAD aggiornato al Decreto Legislativo 13 dicembre 2017, n. 217

"garantiscono l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le Linee guida. A tal fine, ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione

digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità".

L'AgID, secondo l'articolo 51 del CAD aggiornato al Decreto Legislativo 13 dicembre 2017, n.217

"attua, per quanto di competenza e in raccordo con le altre autorità competenti in materia, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica. AgID, in tale ambito:
a) coordina, tramite il Computer Emergency Response Team Pubblica Amministrazione (CERT-PA) istituito nel suo ambito, le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
b) promuove intese con le analoghe strutture internazionali;
c) segnala al Ministro per la semplificazione e la pubblica amministrazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni."

Secondo osservatori.net

"L'Italia mostra miglioramenti nell'attuazione dell'Agenda Digitale, ma nei Digital Maturity Indexes è ancora terzultima in Europa per fattori abilitanti e quartultima per risultati raggiunti".

Possiamo quindi considerare l'Italia come un paese che ha una crescita digitale molto lenta rispetto ad altri paesi europei.

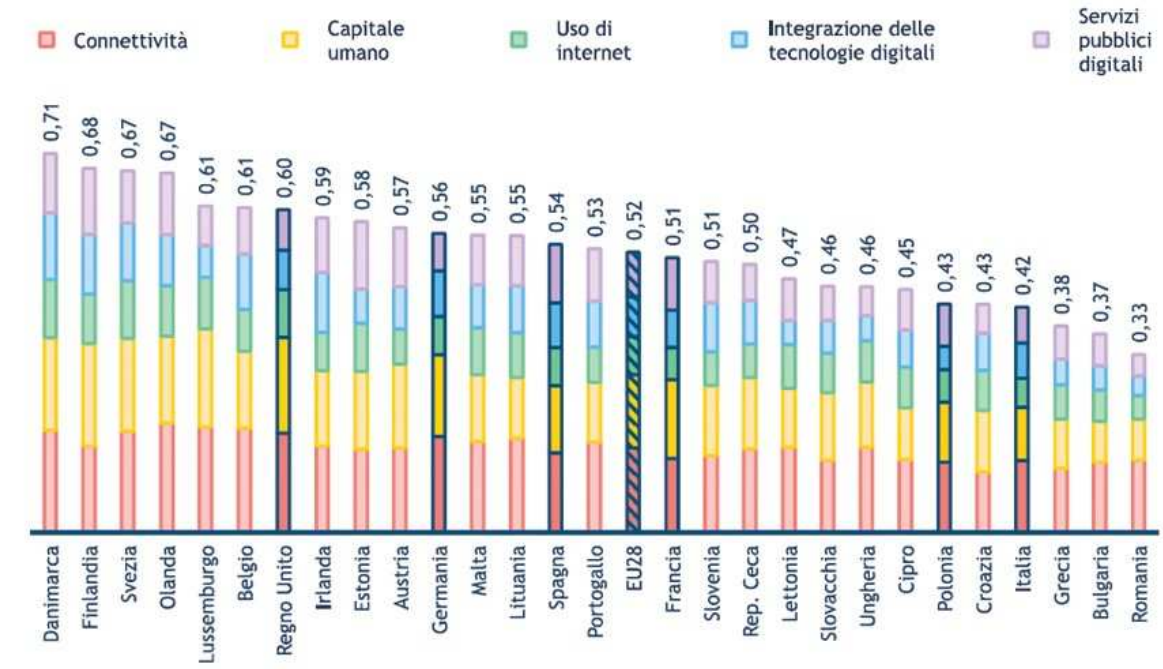


Figura 1.1. *Posizionamento dei Paesi europei sul DESI 2017 (relativo a dati di metà 2016)*[2]

Fonte: osservatori.net

Sempre citando la stessa fonte

> *"Solo il 26% dei cittadini usa esclusivamente canali digitali per fruire di servizi pubblici. Il 60% vorrebbe sistemi che gestiscano automaticamente le loro esigenze".*

e inoltre

> *"Dal 2013 al 2015 la PA italiana ha speso mediamente 5,6 miliardi di euro l'anno in tecnologie digitali, a fine 2018 la spesa potrebbe diminuire di 500 milioni, liberando risorse per investimenti".*

La responsabilità della PA, secondo AgID

> *"L'adeguamento alle misure minime è a cura del responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie, come indicato nel*

CAD (art. 17) o, in sua assenza, del dirigente designato. Il dirigente responsabile dell'attuazione deve compilare e firmare digitalmente il "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017".

L'AgID ha stabilito delle misure minime di sicurezza utili specialmente per le realtà più piccole perché queste hanno meno possibilità di avvalersi di professionisti del settore.

Le misure minime secondo l'AgID

"

- *forniscono un riferimento operativo direttamente utilizzabile (checklist),*
- *stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili;*
- *forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento;*
- *responsabilizzano le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica."*

Secondo l'AgID ci sono tre livelli di attuazione delle misure minime a seconda della complessità del sistema informativo

"

- *Minimo: è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.*
- *Standard: è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.*
- *Avanzato: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni."*

Nel 2017 è stato creato un Piano Triennale per l'Informatica nella Pubblica Amministrazione con la collaborazione tra l'AgID e il Team per la Trasformazione Digitale, per il

triennio 2017-2019.
È stato creato anche il piano 2019-2021, un documento di più di 300 pagine avente come capitoli

1. Il Piano Triennale per l'informatica nella Pubblica Amministrazione
2. Contesto normativo europeo e nazionale
3. Infrastrutture
4. Modello di interoperabilità
5. Dati della Pubblica Amministrazione
6. Piattaforme
7. Ecosistemi
8. Sicurezza informatica
9. Strumenti per la generazione e la diffusione di servizi digitali
10. Modelli e strumenti per l'innovazione
11. Governare la trasformazione digitale
12. Razionalizzazione della spesa ICT della PA
13. Indicazioni per le pubbliche amministrazioni

Il Piano triennale 2019-2021 prevede 126 risultati da produrre nell'arco del triennio: 69 di questi andavano conseguiti entro il 2019. Alla fine dell'anno, ovvero nove mesi dal rilascio del Piano, ne sono stati raggiunti 40. Questo è ciò che risulta dall'analisi dell'Osservatorio Agenda Digitale del Politecnico di Milano.

4.2 Situazione aziende

Le aziende trattano oggi molte quantità di dati. La protezione e l'uso dei dati è regolamentata dal nuovo Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Questi dati devono essere adeguatamente protetti. Le aziende adottano quindi diverse metodologie per avere i dati sempre protetti e disponibili. La preoccupazione riguardo i dati e le infrastrutture non sono un argomento nuovo, considerando che esiste un articolo del 1984 del Jurimetrics Journal che dice

> *"Increasing computer dependence has caused the business community to seek ways to minimize risks of data center failures. Several approaches have evolved, including "Clubs," reciprocal agreements and third-party computer backup agreements. The agreements contain many important provisions unique to computer backup arrangements, and counsel must ensure his or her client's interests are served and protected".*

In questo articolo si parla anche di accordi per minimizzare il rischio di fallimento dei data center e accordi per i backup. Sorprende il fatto che già negli anni '80 fosse già fondamentale evitare la perdita di dati

> *"Many major corporations would be out of business in a week or less, if they lost their data processing center". (Jurimetrics Journal, 1984)*

Inoltre, sempre nello stesso articolo

> *"The increasing computer dependence of our society has been well documented elsewhere. The risks and dangers of computer failure will only increase as more and more commercial applications are automated, as the processing of information is taken out of the hands of humans and placed in the disk storage and tape drives of a computer".*

Ad oggi, le soluzioni di Disaster Recovery per i privati sono diventate molto più facili da usare ed economiche. La nascita dei diversi servizi di backup su cloud a basso prezzo ha permesso a molte aziende di avere delle maggiori possibilità di recupero dati in caso di disastro. I piani di Disaster Recovery risultano molto utili per il recupero dei dati in seguito ad un disastro. Esistono diversi piani di Disaster Recovery, dai più semplici ai più

complessi. Le aziende più grandi non solo hanno un piano di Disaster Recovery ma anche un piano di business continuity. Cioè non hanno solamente un piano per stabilire cosa fare in caso di disastro ma anche un piano per assicurare il più possibile la continuità dei servizi aziendali. I piani di Disaster Recovery più complessi possono comprendere anche la gestione con i media, la gestione dei contatti con i familiari, le polizze assicurative, le azioni legali e altro. Ci sono aziende che hanno ottenuto la certificazione ISO 22301 (Business Continuity Management). Questo significa che ci sono standard di elevata qualità e complessità che le aziende, anche italiane, possono seguire. Possiamo ritenere che il grado di complessità del piano di Disaster Recovery debba essere proporzionato al settore e alla grandezza della azienda. Inoltre, è importante anche valutare l'importanza dei dati che vanno protetti quando si redige il piano di Disaster Recovery. È importante ricordare che il piano deve essere anche testato ed aggiornato, così da assicurarsi il suo funzionamento.

Capitolo 5

Caso Bitways S.r.l.

5.1 Storia dell'azienda

Da Mirko Guerra, il Responsabile Legale di Bitways

> *"Rappresenta il coraggio e la passione di un gruppo di tecnici informatici che hanno riunito le loro competenze, per proporsi sul mercato con un progetto sul tema della tutela della privacy, che rappresenta una delle questioni più importanti nello sviluppo delle piattaforme informatiche. Email, documenti e database sono il principale patrimonio di qualunque azienda ma sono vulnerabili. Bitways si pone a servizio della ricerca di soluzioni sempre più innovative in questo ambito, offrendo ai clienti le migliori opportunità per proteggere i propri dati, mantenendoli al contempo facilmente accessibili su ogni piattaforma e device".*

5.2 Avvenimento

Fonte: ilbuonsenso.net

La notte tra l'8 e il 9 agosto 2019 a Faenza in Via Deruta è andato a fuoco l'edificio in cui risiedeva Bitways. Bitways ha subito un grave danno ed è stata messa alla prova da questo evento. È stato molto importante cercare per Bitways di recuperare i dati nel più breve tempo possibile. Hanno dovuto ricomprare quasi interamente il materiale aziendale, essendo andato praticamente tutto distrutto nell'incendio.

5.3 Tempo di recupero

A circa da 52 ore dall'evento Bitways è stata in grado di far tornare i servizi attivi e le aziende con cui lavorano hanno potuto continuare le loro attività.

5.4 Reazione al problema

Da Mirko Guerra, il Responsabile Legale di Bitways

> *"È stata un'impresa iniziata con la consapevolezza che prima di tutto venivano loro, i nostri clienti. Prima ancora di leccarci le ferite, fare i conti dei danni subiti, di metterci le mani nei capelli, dovevamo mantenere al centro della nostra attenzione i nostri clienti. E così è stato, grazie all'unione e alla forza del Team Bitways di 13 persone, tecnici, commerciali e amministrativi. Tutti - rimarca l'amministratore - si sono rimboccati le maniche e hanno condiviso un solo semplice obiettivo: tutto nuovamente operativo per le 7,30 di lunedì 12 agosto 2019".*

Bitways ha realizzato un video diffuso sui social network, ottenendo risposte di solidarietà e sostegno da parte di molte persone, anche sconosciute. Bitways ha organizzato a settembre 2019 a Faenza un incontro che spiega i lati positivi emersi dall'evento di agosto, in cui erano presenti anche delle istituzioni.
Secondo il Sindaco di Faenza

> *"Per quanto mi riguarda l'incendio, oltre a tante difficoltà, ha messo in luce una grande capacità di lavoro di squadra tra enti, istituzioni e volontari che si è toccata sul campo in quei giorni . Grazie alla sinergia che si è costruita siamo riusciti a contenere danni che altrimenti sarebbero stati ancora più disastrosi".*

Bitways ha deciso di creare una campagna crowdfunding, nata da un brainstorming. Bitways ha ricevuto molto incoraggiamento fin dall'inizio della campagna crowdfunding. Subito dopo l'incendio il CEO (Mirko Guerra) non sapeva come "accettare" il denaro da chi voleva aiutarli, decidendo così di fare una campagna di crowdfunding. Nei mesi Bitways ha partecipato a diversi eventi pubblici e non. La campagna ha permesso di far conoscere a Bitways tanti clienti e imprenditori.

5.5 Campagna crowdfunding

Da "Crowdfunding. Il finanziamento della folla, o dei 'folli'?" di G. Quaranta:

> *"Il crowdfunding è un particolare tipo di finanziamento collettivo che, sfruttando le potenzialità di Internet, consente a coloro che hanno idee o delle necessità, ma – rispettivamente - non i tutti i fondi per realizzarle o soddisfarle, di provare ad accedere a risorse economiche di terzi, partendo da quelle di parenti e amici (family and friends) nella speranza di attrarre anche quelle - molto più ingenti - della folla (crowd) che popola il mondo online, la quale (fools), fidandosi dei meccanismi di feedback che si generano tra gli utenti - come discriminante per la validità e la fattibilità di un progetto -, è disposta a finanziare un numero crescente di idee (bisogni), in quanto la tendenza - trainata da World Wide Web - è quella di vendere sempre più unità di prodotti e/o servizi specifici per piccole nicchie. In questo modo, chiunque può, potenzialmente, accedere ad un vero e proprio 'finanziamento della folla'".*

5.6 Tipologie di crowdfunding

- **Reward-based:** È il modello usato da Kickstarter e Indiegogo. Gli organizzatori offrono un reward a chi dona. Spesso questa tipologia viene usata per finanziare giochi, musica, film, libri. La ricompensa è spesso "non tangibile", come ad esempio un ringraziamento sul sito dell'organizzatore, un ringraziamento sui social o il nome nei titoli di coda. A volte si finanziano anche veri e propri prodotti, come ad esempio cuffie di alta qualità. In questo caso il donatore avrà il prodotto prima della eventuale "vera" immissione sul mercato e ad un prezzo ridotto.

- **Donation-based:** È il modello delle organizzazioni no profit e onlus che cercano persone che credano in loro e nei loro progetti. È una forma molto utilizzata di crowdfunding, a chi dona non viene dato nessun compenso, né materiale né "non tangibile".

- **Lending-based:** In questa tipologia il denaro donato viene dato in prestito agli organizzatori del progetto. I soldi verranno restituiti alla conclusione del progetto. Molte volte il tasso di interesse del prestito è maggiore di quello delle banche.
- **Equity-based:** È il modello ad oggi maggiormente utilizzato dalle startup italiane. Chi dona effettua una sorta di investimento, diventando "socio" dell'azienda. Sostenendo il progetto si va ad "acquistare" una quota dell'azienda che è alla ricerca di denaro.

5.7 La campagna reward-based

Bitways ha creato una campagna crowdfunding con dei rewards per ringraziare chi effettuava delle donazioni. Hanno deciso la modalità tutto o niente, per cui se non avessero raggiunto l'obiettivo non avrebbero ottenuto niente. Oltre alla donazione libera con cui non si otteneva nessun reward, ci sono stati diversi reward proporzionalmente collegati alla donazione.
I rewards sono stati:

- per **10 euro:** Un ringraziamento sui social.
- per **50 euro:** Un decalogo sulla gestione dei dati e Disaster Recovery e un ringraziamento sui social.
- Per **100 euro:** Accesso privilegiato ad un webinar dedicato alla tematica del backup e Disaster Recovery, un decalogo sulla gestione dei dati e Disaster Recovery e un ringraziamento sui social.
- Per **250 euro:** Invito ad un evento che si terrà a Faenza nei primi mesi del 2020 che parla del progetto e per continuare il percorso di sensibilizzazione sulla tematica, accesso privilegiato a 5 webinar dedicati alla tematica della sicurezza dei dati informatici, del backup e Disaster Recovery, un decalogo sulla gestione dei dati e Disaster Recovery e un ringraziamento sui social.
- Per **500 euro:** Consulenza focalizzata sulla corretta gestione dei dati, invito ad un evento che si terrà a Faenza nei primi mesi del 2020 che parla del progetto e

per continuare il percorso di sensibilizzazione sulla tematica, accesso privilegiato a 5 webinar dedicati alla tematica della sicurezza dei dati informatici, del backup e Disaster Recovery, un decalogo sulla gestione dei dati e Disaster Recovery e un ringraziamento sui social.

- Per **1000 euro:** Consulenza e analisi presso la sede dell'azienda donatrice, focalizzata sulla corretta gestione dei dati, invito ad un evento che si terrà a Faenza nei primi mesi del 2020 che parla del progetto e per continuare il percorso di sensibilizzazione sulla tematica, accesso privilegiato a 5 webinar dedicati alla tematica della sicurezza dei dati informatici, del backup e Disaster Recovery, un decalogo sulla gestione dei dati e Disaster Recovery e un ringraziamento sui social.

5.8 Obiettivo

Bitways è riuscita a raggiungere la cifra di 33610 euro su un obiettivo di 30000 euro. Il traguardo è stato raggiunto del 112% con il sostegno di 196 sostenitori.

Fonte: ideaginger.it

5.9 Quali sono state le loro priorità

La loro ripartenza era considerata secondaria rispetto a quella dei loro clienti. Questo perché senza di loro l'azienda non avrebbe potuto tornare operativa.
I dipendenti di Bitways si sono quindi suddivisi i ruoli per la gestione del Disaster Recovery. C'è chi ha gestito la parte tecnica, chi il rapporto con i fornitori, chi ha identificato una sede temporanea e chi ha trattato il rapporto con i clienti.
Dopo essere riusciti a far tornare operativi i clienti si sono concentrati sulla loro azienda. Era necessario quindi identificare una nuova sede, ripartendo da zero.

5.10 Proseguimento post crowdfunding

Dopo aver concluso la campagna, il CEO (Mirko Guerra) e l'IT Manager (Luca Giustra) hanno fatto una live con Marco Zammarchi (che si occupa del marketing di Bitways). Dopo il crowdfunding l'azienda si impegnerà a portare avanti l'importanza dei dati e della loro tutela. Bitways vuole, con la sua esperienza, dare un esempio positivo di come si possa far "rinascere" un'azienda non avendo rimasto praticamente nulla.
Per il 2020 Bitways vorrebbe portare avanti l'importanza dell'IT e dei dati iniziando a svolgere delle attività in diverse forme, mezzi e modalità alternative a quelle solitamente utilizzate dall'azienda.
Bitways ha l'idea di creare una community con l'intenzione di realizzare live e webinar legati al settore di Bitways. Bitways ha anche dei supporter fisicamente non vicini e il web renderebbe la comunicazione molto più facile e flessibile. Probabilmente Bitways fisserà un appuntamento a marzo 2020 per proseguire nel percorso di divulgare l'importanza della gestione e della tutela dei dati. Considerando i danni provocati dall'incendio, Bitways cercherà comunque di essere positiva e trarne vantaggio.

Capitolo 6

Configurazioni RAID

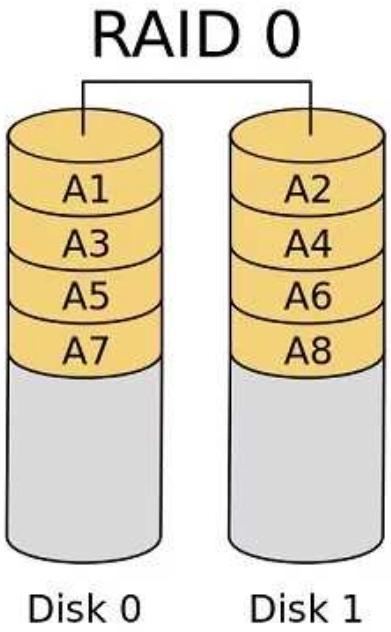
Considerando l'evoluzione di nuove tipologie di dischi e l'aumentare della capacità dei dischi, oggi non c'è più bisogno di utilizzare molti dischi contemporaneamente. Le nuove tecnologie hanno permesso a parità di prezzo di diminuire il costo e aumentare capacità e velocità.
Anche se ci sono stati molti miglioramenti tecnologici negli ultimi anni, si rende comunque necessario l'uso di strategie in grado di ridurre al minimo il rischio di perdere dati preziosi.
RAID deriva dall'acronimo in inglese di Redundant Array of Indipendent Disks. Nella pratica il RAID indica una tecnica che permette di gestire le diverse unità di archiviazione collegate tra loro. Questa tecnica divide i dati nei dischi così da riuscire ad aumentare le prestazioni, la sicurezza e anche la tolleranza ai guasti.
Le tipologie RAID di base vanno da 0 a 7, esistono poi anche delle tipologie RAID annidate che si ottengono combinando tra loro delle combinazioni RAID di base.

6.1 Come si usa il RAID

Il RAID è legato all'utilizzo di un controller. Questo viene spesso integrato nelle schede madri dei sistemi oppure viene integrato tramite una scheda esterna. Esiste gestire il RAID anche solamente tramite software. Il RAID software non offre però le stesse prestazioni del RAID hardware.
Il RAID hardware è preferibile perché ha della memoria RAM dedicata e un processore dedicato che esegue i calcoli, piuttosto che avere hardware condiviso. Alternativamente

al RAID hardware ci sono le soluzioni cloud, spesso economicamente più convenienti. Inoltre, il RAID hardware non è protetto dall'esterno tanto quanto il cloud.

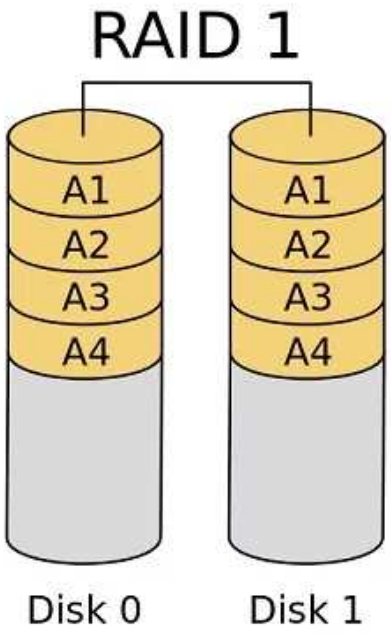
6.2 RAID 0



Fonte: informaticapertutti.com

La tipologia RAID di livello 0 divide i dati in blocchi identici. Ognuno di essi viene poi scritto su un disco diverso. In questo caso per realizzarlo servono almeno due dischi. La capacità effettiva è data dalla capacità del disco di dimensioni minori moltiplicata per il totale dei dischi.
Come vantaggi ci sono la facilità di implementazione e le prestazioni circa proporzionali al numero di dischi impiegati. Il problema sta nel fatto che questo non è proprio un RAID perché non offre nessuna protezione contro i guasti. Il RAID 0 è indicato per il caricamento di programmi che usano grandi quantità di dati ma è meglio evitare nei casi in cui la sicurezza è prioritaria.

6.3 RAID 1

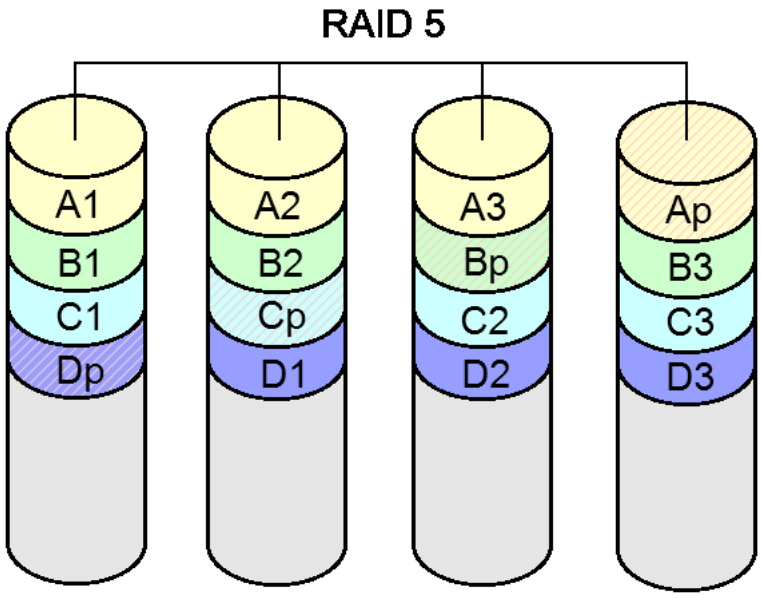


Fonte: informaticapertutti.com

Il RAID 1 viene anche chiamato mirroring. Questo perché il contenuto viene scritto sul disco primario, poi viene replicato su uno o più dischi secondari. In questa tipologia di RAID è necessario usare almeno due dischi e la capacità utilizzabile è solamente la capacità del disco con dimensioni minori. Viene ammesso il guasto di tutti i dischi tranne uno. Il RAID 1 è una delle configurazioni RAID più semplici ed assicura la replica dei dati e la tolleranza contro i guasti. Nel caso in cui un disco si rompesse, basta sostituirlo. Un altro vantaggio è dato dal fatto che c'è un leggero miglioramento delle prestazioni in lettura, perché il controller potrebbe fare simultaneamente più letture.
Il RAID 1 ha un enorme svantaggio dato dal fatto che ha una pessima gestione dello spazio disponibile. Inoltre, dato che bisogna scrivere i dati contemporaneamente su tutti i dischi, le prestazioni in scrittura non miglioreranno rispetto all'utilizzo di un unico disco. Il RAID 1 è consigliabile quando è di massimo importanza la continuità del servizio.

6.4 RAID 5

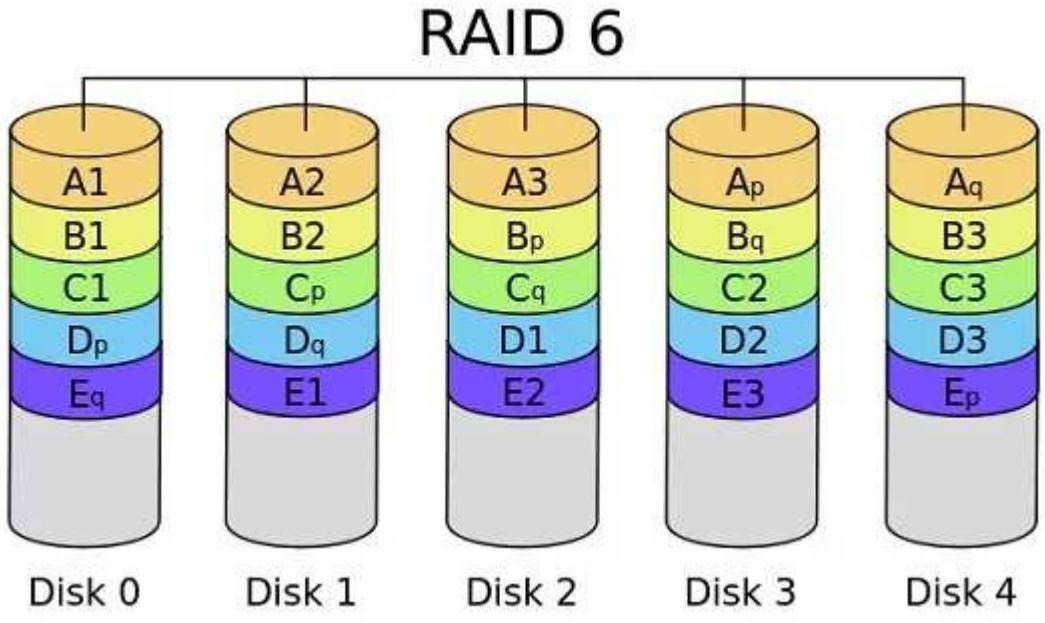
Con la descrizione del RAID 5 si introduce un altro importante elemento nella gestione dei dati, il bit di parità. Grazie all'utilizzo del bit di parità, il RAID 5 può essere consigliato per qualsiasi utilizzo.



Fonte: Wikipedia

Il RAID 5 è in grado di offrire sia un aumento delle prestazioni sia una maggiore sicurezza sui dati. In questo caso il numero minore di dischi è tre. La capacità effettiva è uguale a quella del disco di dimensioni minori moltiplicata per il numero totale dei dischi meno uno.
Esiste la possibilità di scrivere e leggere su più di un disco contemporaneamente. Inoltre, le prestazioni aumentano in base al numero di dischi utilizzati. Anche se è buona la velocità in lettura e scrittura, nel caso di rottura di un disco, le prestazioni generali ne risentiranno. Sempre in caso di rottura del disco il ripristino dell'intero RAID 5 può richiedere molto tempo.

6.5 RAID 6



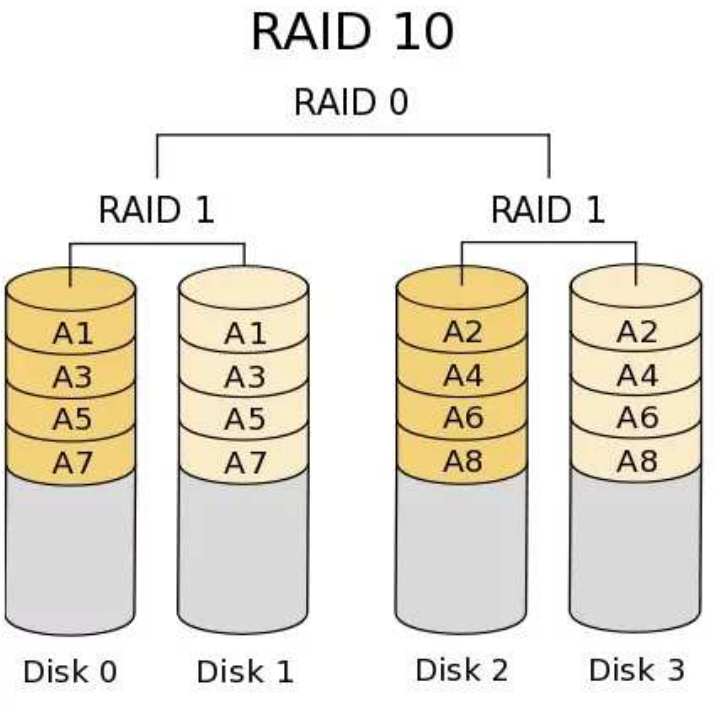
Fonte: informaticapertutti.com

Il RAID 6 è molto simile al RAID 5, però usa due dischi per la parità dei dati al posto di uno. Così facendo, l'intero sistema sopravvive anche al guasto di due dischi contemporaneamente.
Il numero minimo di dischi sale in questo caso a quattro. La capacità effettiva è uguale a quella del disco di dimensioni minori moltiplicata per il numero totale dei dischi meno due. Come nel RAID 5, anche nel RAID 6 il danneggiamento di un disco influisce negativamente sull'intero sistema e anche in sto caso il ripristino potrebbe richiedere molto tempo.

6.6 RAID annidati

Come descritto precedentemente, si possono utilizzare anche configurazioni RAID sommate tra loro. La tipologia di RAID viene descritta scrivendo un numero con le cifre dal livello più nidificato a quello più esterno.

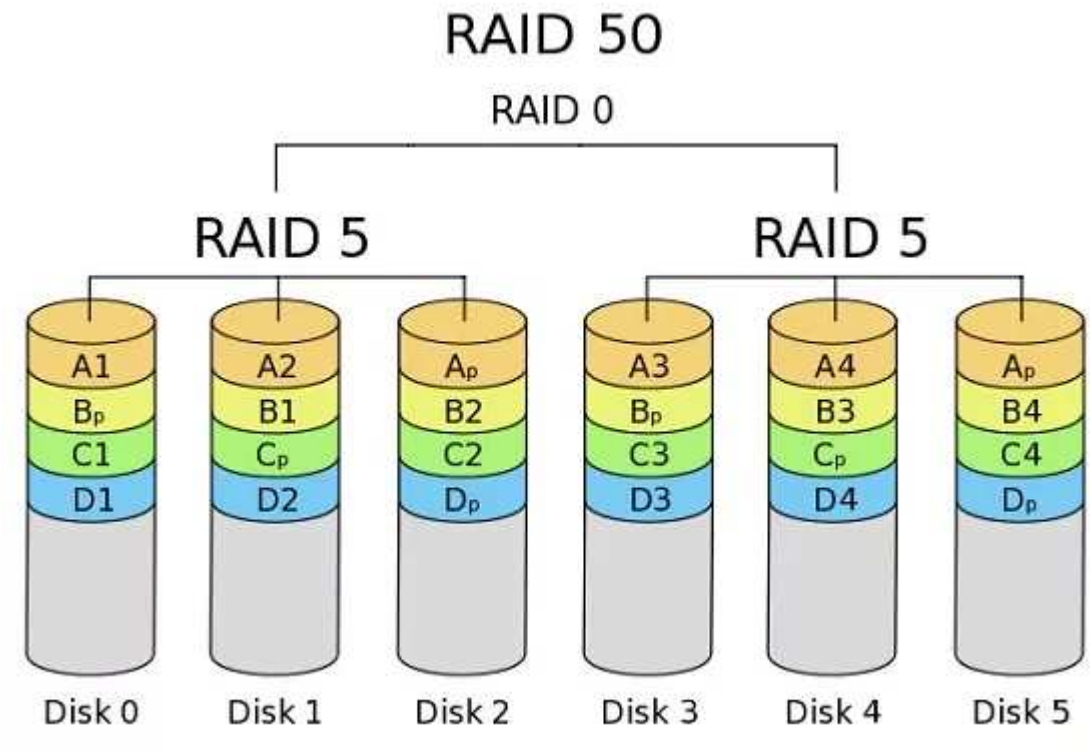
6.6.1 RAID 10 (1+0)



Fonte: informaticapertutti.com

È la configurazione più semplice di RAID annidata. Grazie all'utilizzo di questa struttura, il RAID consente di avere delle ottime prestazioni. È quindi ottimo per applicazioni che richiedono buone prestazioni e contemporaneamente tolleranza ai guasti. Nel RAID 10 servono almeno quattro dischi. La capacità effettiva è uguale a quella del disco di dimensioni minori moltiplicata per il numero totale di dischi presenti, dividendo il tutto per due.
Prendendo a confronto il RAID 10 e il RAID 0, il RAID 10 ha una tolleranza ai guasti decisamente maggiore rispetto al RAID 0. Invece, paragonando il RAID 10 con il RAID 5, il RAID 10 non necessita di nessun particolare calcolo per salvare i dati. Sempre in questo caso, il RAID 10 non risente della rottura di un disco quanto il RAID 5.

6.6.2 RAID 50 (5+0)



Fonte: informaticapertutti.com

In questo caso il numero minimo di dischi è sei, quindi due rami con il numero minimo di dischi delle configurazioni RAID 5.
Consideriamo D la capacità del disco di dimensioni minori, N il numero dei dischi ed R il numero di rami. La capacità effettiva è uguale a D x (N/R-1) x R. Esiste creare anche altre configurazioni RAID annidate oltre a quelle presentate.
Anche se le soluzioni annidate consentono la rottura di uno o più dischi, bisogna provvedere nel caso di rottura ad una rapida sostituzione dato che la ricostruzione potrebbe richiedere molto tempo. Per evitare di mettere il sistema a rischio sarebbe utile fare copie di backup a intervalli di tempo regolari.

Capitolo 7

Backup

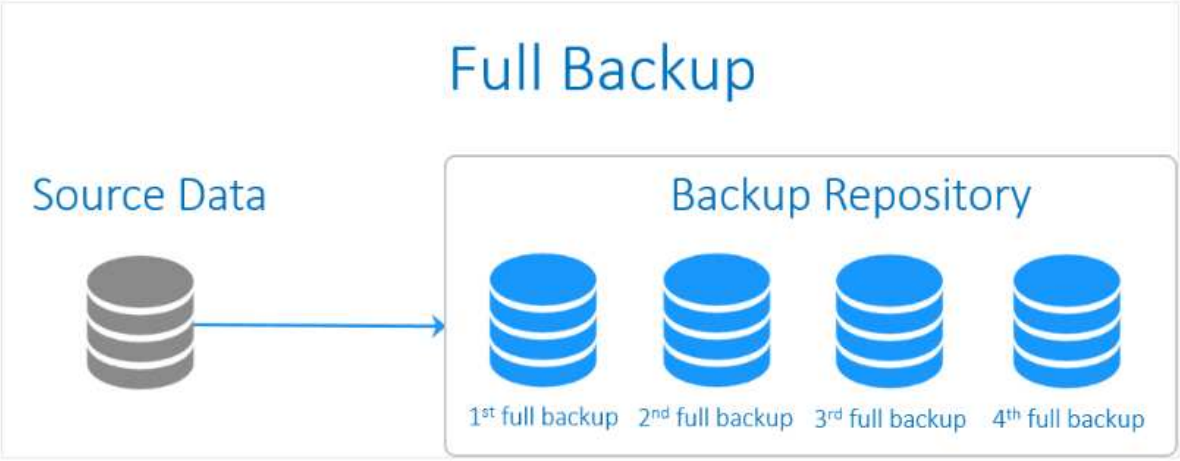
L'evoluzione degli ambienti legati all'informatica tende ad alzare le aspettative in termini di disponibilità e servizi.Le aziende tendono a collezionare grandi quantità di dati ma ciò deve essere integrato con una corretta classificazione e analisi. L'informatica nel campo dei dati porta a creare o adottare soluzioni nuove e innovative rispetto ad usare sistemi già esistenti.
Queste soluzioni per scelta o disponibilità economica non sempre vengono effettuate. Si sta cercando sempre di più di portare le infrastrutture ad un livello basato interamente sul cloud. Questo porta a una riduzione delle complessità delle infrastrutture IT e contemporaneamente permette all'IT di impegnarsi in lavori impostati sul business.
Con l'uso ormai massiccio dei servizi cloud è importante saper adottare le giuste strategie per la sicurezza dei dati aziendali. Bisogna però stare attenti a non entrare in conflitto con altre tecnologie usate dall'impresa.

7.1 Tipologie di backup

7.1.1 Giornaliero

Backup in cui vengono salvati tutti i file modificati del giorno stabilito.

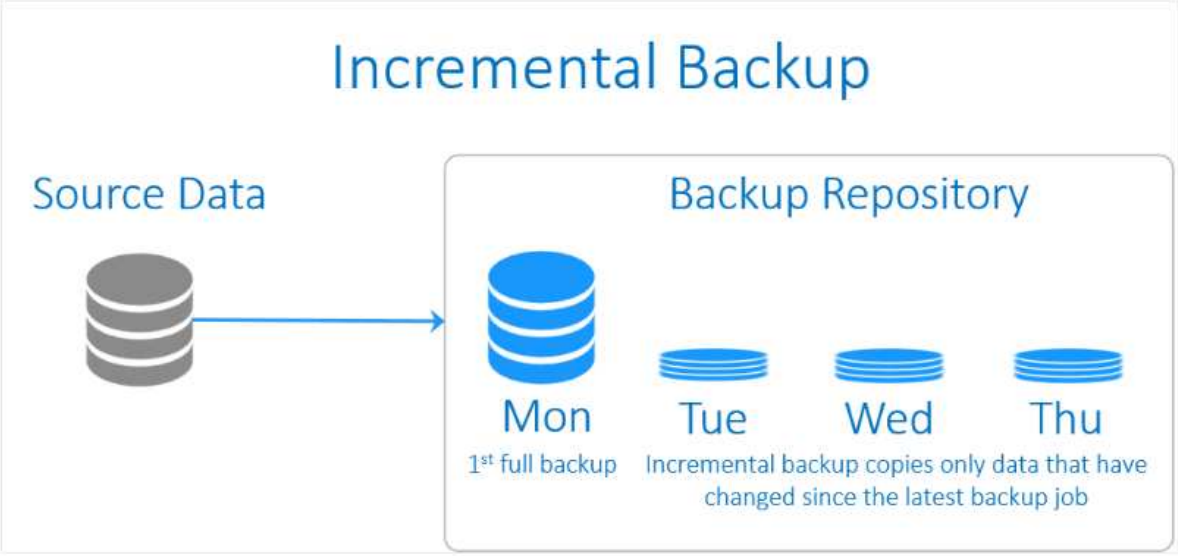
7.1.2 Completo



Fonte: www.nakivo.com

Vengono copiati tutti i file presenti nel sistema. Con un nuovo backup i file saranno sovrascritti perché copiati interamente da zero. Esiste la possibilità di tenere più copie del backup completo.

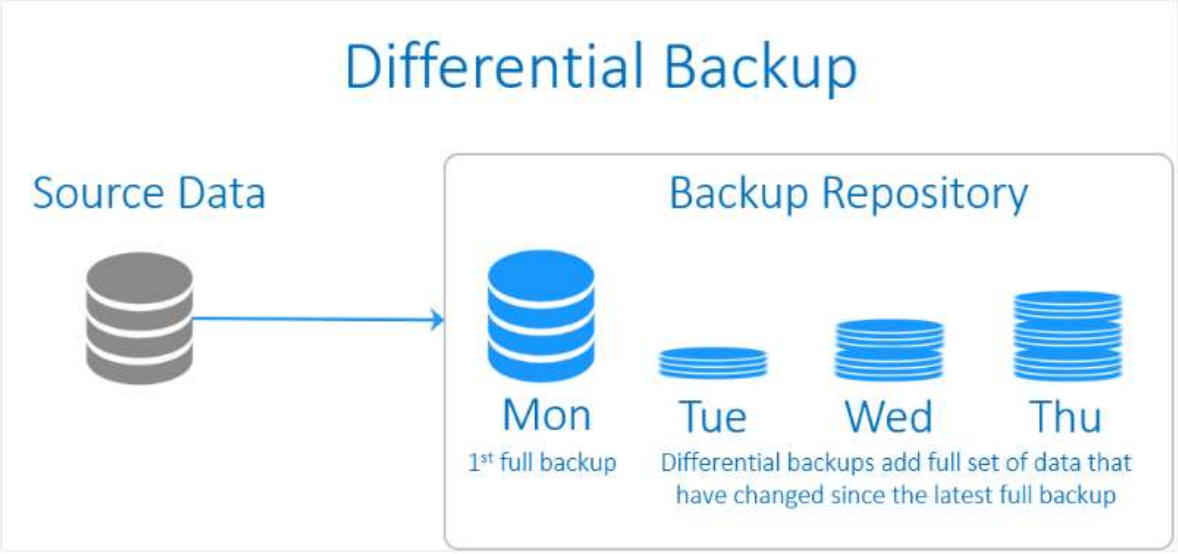
7.1.3 Incrementale



Fonte: www.nakivo.com

Il primo backup è in realtà un backup completo. Dopo questo backup si andranno a creare dei backup in cui saranno presenti solamente le modifiche effettuate ai file. Queste modifiche vengono considerate dall'ultimo backup completo o incrementale. Il ripristino dei file si esegue con il backup completo e tutti i backup incrementali.

7.2 Differenziale

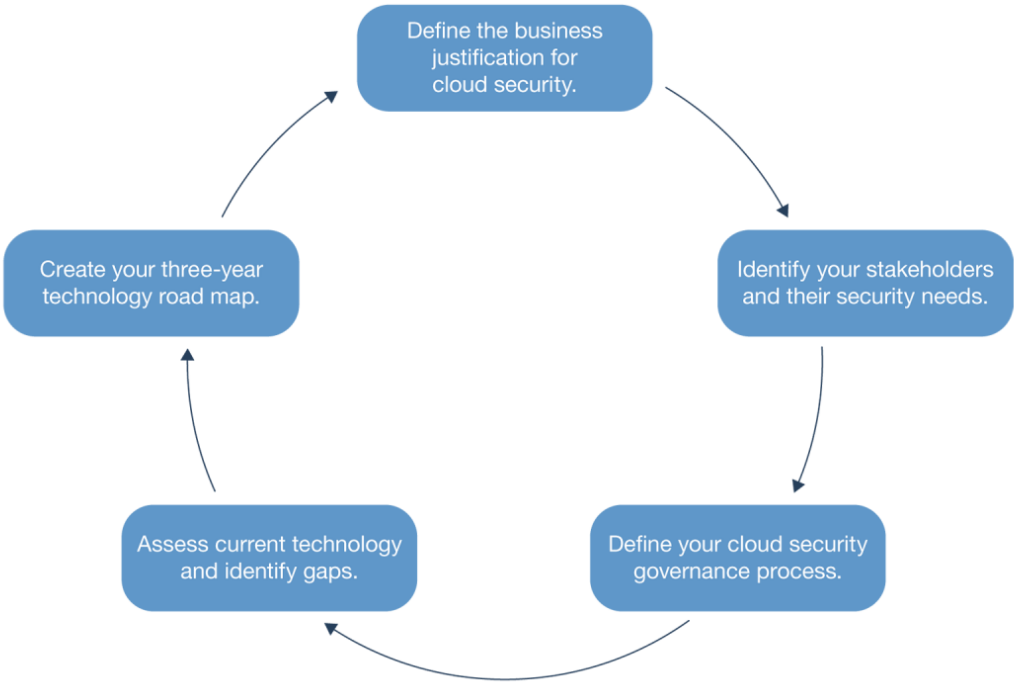


Fonte: www.nakivo.com

Il primo backup è un backup completo. I backup successivi conterranno tutti i file nuovi o modificati rispetto al backup completo. Il ripristino dei file si esegue prendendo il backup completo e l'ultimo differenziale.

7.3 Security Strategy Life (Forrester)

I 5 passi per la sicurezza nel cloud secondo gli esperti di Forrester.



Fonte: Forrester

1. **Raccolta degli elementi che giustificano l'investimento nella sicurezza in cloud**
   Uno dei problemi della security è che non si identifica facilmente se non quando non è funzionante o ci sono grandi perdite di dati. L'investimento è pensato in base alle necessità, diverse per ogni azienda. Questo serve per avere un buon controllo dei dati che porta ad avere dei vantaggi.

2. **Identificazione dei team aziendali per i quali l'uso del cloud è importante e la sicurezza più critica**
   In questa fare si identificano i requisiti e le soluzioni di security che non ostacolino il lavoro dei dipendenti. Bisogna stare attenti a rispettare i requisiti di legge. Sono molto utili i report sugli attacchi informatici e/o sulle perdite di dati. Esistono anche servizi di security, utili per il costante aggiornamento. Questi servizi posso essere considerati positivamente dai team di sviluppatori.

3. **Governo del processo di cloud security**
   Serve controllare che la security dia accesso ai diversi servizi cloud da qualsiasi

tipologia di dispositivo. Vanno solitamente inclusi gli smartphone dei dipendenti, quando si connettono sia dall'interno sia dall'esterno della rete aziendale. Occorre classificare i dati aziendali in base alla criticità degli stessi. Bisogna inoltre istruire i dipendenti a non utilizzare in maniera eccessiva il cloud storage pubblico. È necessario poter aggiornare in maniera veloce e corretta le policy aziendali che riguardano il cloud. Questi aggiornamenti vengono effettuati in base alle leggi vigenti. È importante sapere dove i provider cloud mettono i dati aziendali, questo risulta utile ad esempio per rispettare i requisiti del GDPR. Occorrono inoltre dei sistemi efficaci di sicurezza per identificare eventuali intrusioni nella rete da parte di soggetti non autorizzati.

4. **Rilevazione della situazione esistente per ciò che riguarda la sicurezza in cloud e l'esame delle differenze rispetto a quanto occorre**
   Occorre capire come sono gestiti i dati relativi agli utenti. Inoltre, bisogna osservare come la security incide sull'uso delle applicazioni e dei servizi da parte degli utenti. È importante valutare quanto la security rallenti o impedisca le operazioni di estrazione, trasformazione e caricamento dei dati.

5. **Creazione di una strategia efficace che ottenga il supporto del management**
   È importante riuscire a giustificare le azioni prese basandosi sulle componenti di security osservate. Bisogna inoltre definire un piano temporale di attività della durata di qualche anno. È utile tenere traccia delle scelte effettuate, dei risultati ottenuti e delle problematiche create.

Capitolo 8

Il cloud

> *"Nell'epoca del cloud as a commodity, insomma, migrare le proprie operazioni sulla nuvola non va visto come un costo, né come una preoccupazione. Al contrario: si tratta di un passo necessario per dare alla propria azienda quella marcia necessaria a emergere in un panorama sempre più competitivo, e che consente di concentrarsi al 100% sul proprio business anziché sugli aspetti tecnici che lo mantengono operativo. Questo vale tanto per le aziende di grandi dimensioni ben indirizzate, quanto per le startup – che molto più di frequente – sono native in cloud".*

Stefano Sordi, CMO Aruba S.p.A.

Il cloud ora è per tutti, non solo per grandi aziende ma anche per piccole realtà.

Il cloud ha dato la possibilità a qualunque attività di informatizzare i propri processi senza particolari sforzi e con costi molto contenuti. Le aziende più piccole hanno potuto togliere datacenter costruiti da soli e i relativi software che comportavano un costo non indifferente.

A parte alcuni casi non serve più ospitare "in casa" i datacenter. I costi di manutenzione e gestione delle infrastrutture fisiche sono decisamente più alti rispetto a soluzioni cloud equivalenti. La scalabilità, la versatilità e i costi contenuti rendono il cloud preferibile a qualunque alternativa.

Sfruttare soluzioni cloud permette alle aziende di rimanere operative o tornare operative in poco tempo. Questo anche dopo gravi catastrofi.

Secondo una ricerca effettuata da Kaspersky Lab, quasi due PMI su tre si avvalgono di

una o più applicazioni aziendali che forniscono servizi. Questa tipologia di applicazioni è particolarmente adatta per le aziende con un numero di dipendenti inferiore a 250. C'è una crescita e una migrazione verso i servizi cloud e le aziende sono contente dei servizi offerti dal cloud.
L'uso di servizi cloud è in aumento, il 73% delle medie imprese e il 56% delle piccole imprese utilizzano almeno un servizio cloud.

8.1 Tipologie di servizi cloud

La rivoluzione digitale sta ancora portando a grandi cambiamenti nelle aziende. Le aziende stanno prendendo confidenza e imparando ad usare i nuovi servizi offerti da internet e in particolare dal cloud.

Fonte: aruba.it

8.1.1 IaaS (Infrastructure as a service)

Non si tratta più di infrastrutture private che risiedono nel proprio ambiente lavorativo ma che risiedono in altri luoghi proposti dal provider fornitore di servizi cloud.
IaaS offre un'infrastruttura facilmente scalabile in base alle proprie esigenze e il cliente

paga in base a ciò che usa. Si può quindi "affittare" RAM, CPU e storage in base al bisogno. L'azienda non ha più il bisogno di avere un'infrastruttura IT fisica ma si affida al provider per le macchine e il loro aggiornamento. Il cliente che "affitta" l'infrastruttura decide il sistema operativo e gli applicativi da inserire all'interno.
AWS domina il mercato di questi servizi da quando ha iniziato nel 2006. Microsoft ha comunque cercato di raggiungere AWS proponendo nuovi servizi. Inoltre, Google ha iniziato a creare i propri servizi cloud pubblici.

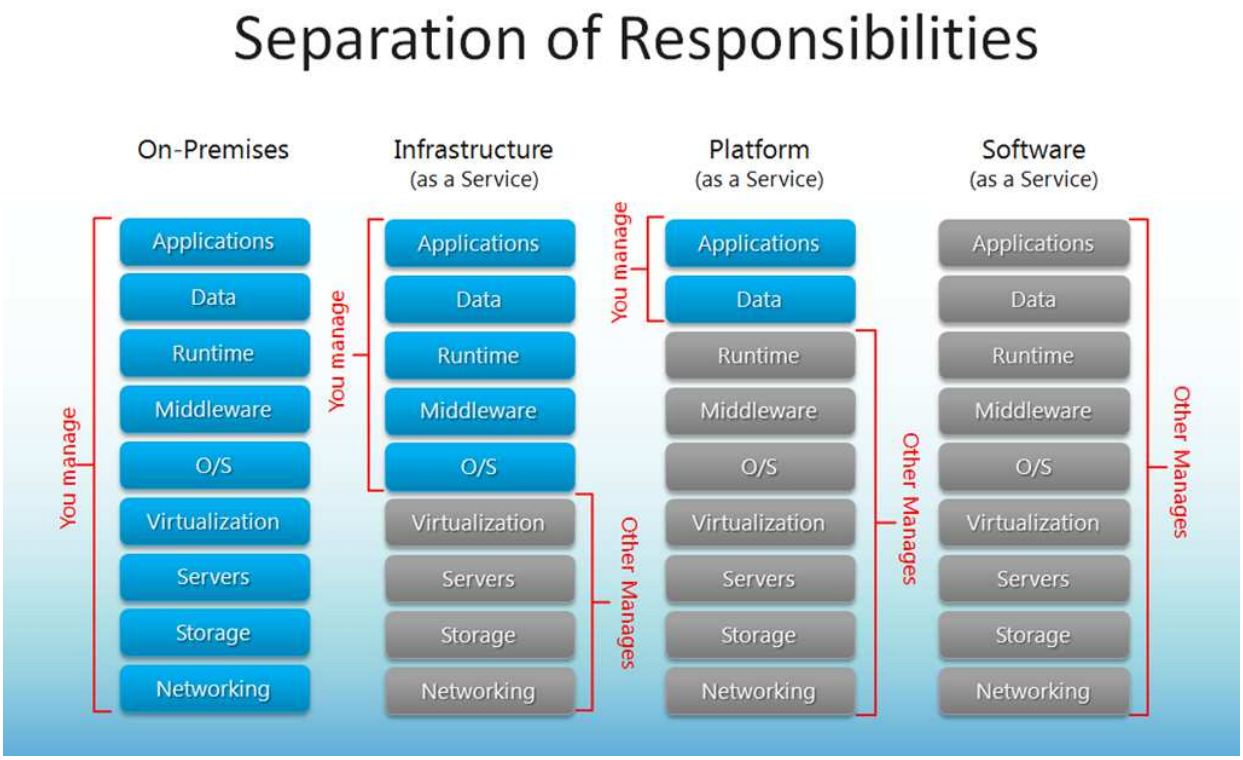
8.1.2 PaaS (Product as a service)

Si possono "noleggiare" una serie di middleware come i database per creare delle applicazioni da far girare su cloud. Si richiede al provider uno spazio in cui sviluppare e distribuire le applicazioni.
Per fare questo non è necessario installare sistemi operativi o ambienti di sviluppo perché viene tutto gestito dal provider che offre il servizio.

8.1.3 SaaS (Software as a service)

I software cloud sono ampiamente conosciuti da tutti. Ad esempio Gmail, Google Drive, Office 365.
Lo scopo dei SaaS è fornire ad utenti sia aziendali sia privati delle applicazioni accessibili ovunque via web. I software e i dati risiedono nei server del provider che fornisce il servizio. Non c'è quindi la necessità di memorizzare i dati fisicamente nell'azienda o in casa.
L'utilizzo delle applicazioni è molto facile e veloce, ad esempio accedendo da browser. C'è il pagamento di un canone per l'utilizzo del software senza preoccuparsi di installazioni varie e di dover gestire delle macchine fisiche.
Molte persone utilizzano i SaaS ogni giorno per lavorare a documenti, presentazioni, grafiche e anche sui gestionali. Le possibilità sono molto vaste dato che ormai molti software sono caricabili su macchine virtuali.

8.2 Responsabilità nei diversi tipi di servizio



Fonte: opencloudict.it

8.3 Vantaggi del cloud

Il cloud è una tecnologia che consente all'utente di accedere tramite internet ai propri dati e servizi.

> *"L'Italia si rivela un Paese molto ricettivo, dove il business cloud continua a crescere a due cifre con un fatturato anno su anno quasi raddoppiato".*

V. Esposito, Direttore divisione PMI e Partner Microsoft Italia

Il 50% delle aziende con meno di 50 dipendenti hanno dipendenti che lavorano regolarmente fuori dall'ufficio e che hanno bisogno di accedere ai dati e alle applicazioni tramite cloud.

Nexive, il più grande operatore postale privato d'Italia, ha deciso di passare al cloud,

portando le proprie operazioni di front-end e back-end (come le soluzioni di recapito postale e i prodotti di e-commerce) nel Global Cloud Data Center di Aruba.
Di seguito alcuni dei principali vantaggi dati dal cloud.

- **Abbattimento dei costi hardware e software**
  Si riesce a ridurre in maniera considerevole l'uso di hardware e software. Questo dato dal fatto che l'azienda non si trova dove si trovano i dati. Il provider mette a disposizione il suo hardware e software che altrimenti sarebbero da acquistare e collocare fisicamente nel luogo dove si trova l'azienda. L'azienda da remoto riesce a sfruttare le infrastrutture del provider in cui vengono collocati dati e servizi.

- **Abbattimento dei costi per manutenzione e aggiornamento**
  La manutenzione e l'aggiornamento dei sistemi non sono a carico dell'azienda ma dal provider. L'azienda può avere dei servizi sempre aggiornati senza particolari preoccupazioni. Inoltre, consente anche di investire meglio tempo e denaro che sarebbe altrimenti utilizzato per gli aggiornamenti.

- **Abbattimento dei costi per l'energia elettrica**
  Non avendo server situati nel luogo in cui si lavora, l'azienda non deve pagare il consumo di energia elettrica necessario per alimentare i server.

- **Abbattimento dei costi per spreco di risorse**
  Il cloud permette di pagare soltanto per ciò che si utilizza e modificare in maniera veloce ed efficace le risorse. Il numero di server può aumentare o diminuire in maniera molto semplice, così come RAM, CPU e lo storage disponibili per ogni server.

- **Riduzione dei rischi**
  La sicurezza dei dati e dei sistemi è a carico del provider. Il provider adotta le misure necessarie per la protezione dei dati e utilizza software sempre più aggiornati e sicuri. I backup sono gestiti automaticamente dal provider senza intervento da parte dell'azienda.

- **Accesso ai dati e servizi ovunque**
  L'azienda può utilizzare i suoi dati e servizi ovunque avendo una connessione ad internet.

- **Alta affidabilità garantita**
  La disponibilità del servizio è garantita da contratto e ha un valore medio pari al 99,9%. Con dei server presenti nel luogo dell'azienda questo obbiettivo non è raggiungibile con scarsi investimenti economici.

8.4 Svantaggi del cloud

Senza le giuste soluzioni di cyber security i sistemi cloud possono essere a rischio. Senza di esse c'è una mancanza di controllo della sicurezza delle applicazioni aziendali e dei dati dei clienti. L'uso del cloud ha anche dei risvolti negativi. Le infrastrutture IT stanno utilizzando più servizi ma non sempre si ha il controllo su di essi.
Secondo uno studio di Kaspersky Lab, il 66% delle aziende da 1 a 149 dipendenti non riesce a gestire facilmente le infrastrutture IT eterogenee. Viene quindi richiesto di avere un nuovo approccio per la gestione delle infrastrutture IT. Il problema sta anche nel fatto che gli addetti all'IT di un'azienda non sempre sono sufficientemente competenti nella gestione delle infrastrutture.
Inoltre, il 14% delle aziende tra i 50 e 249 dipendenti si rivolge a figure professionali non specializzate per curare la sicurezza delle proprie infrastrutture IT. C'è quindi un rischio reale per la cyber security aziendale. La perdita o l'accesso non autorizzato ai dati aziendali e a quelli dei clienti porterebbe a gravi danni reputazionali, non sempre facilmente risolvibili. Da ciò potrebbero facilmente aggiungersi danni economici causati da problemi legali.
È perciò utile proteggersi adeguatamente. Inoltre, sarebbe opportuno fornirsi di specialisti nel campo della sicurezza informatica evitando personale non adeguatamente preparato e qualificato. Oppure, è possibile scegliere di formare dei dipendenti già presenti in azienda che si occuperanno della cyber security.

8.5 Esempio servizio cloud: Office 365

La versione online delle applicazioni Microsoft è stata ideata per gli utenti che vogliono tagliare dei costi relativi al software aziendale e migliorare la propria efficienza. La suite Office 365 consente all'utente di lavorare ovunque ci sia una connessione ad internet e

in maniera sicura, grazie alle tecnologie di protezione presenti nel software in cloud. Gli aggiornamenti sono eseguiti automaticamente, per cui si dispone sempre della versione più aggiornata e sicura.
Nei servizi di Office 365 che un utente può utilizzare ci sono, ad esempio

- **Exchange:** posta elettronica, contatti, calendario
- **Skype for Business:** chat, chiamate audio/video, conferenze
- **SharePoint:** gestione e condivisione di documenti
- **Teams:** chat e condivisione file

8.6 Esempio servizio cloud: Microsoft Azure

Microsoft Azure è l'ambiente cloud di Microsoft, questo servizio serve per spostare al di fuori dell'azienda i propri dati e servizi. Questi saranno ospitati sui server appartenenti a Microsoft, con dei risparmi economici per l'azienda.
I tempi per l'implementazione sono ridotti rispetto ad avere l'infrastruttura IT in azienda. L'azienda può personalizzare il tipo di macchina, i sistemi e i servizi in base ai propri bisogni. Il suo modello è basato sul "pay-per-use", l'azienda pagherà quindi a consumo. Essendo una piattaforma facilmente gestibile e flessibile, l'azienda sceglie quali e quante risorse utilizzare in base a quello che necessita al momento.
Inoltre, esiste la possibilità di gestire una sorta di eventi, quando questi eventi si "attivano" le funzionalità verranno cambiate automaticamente. Nel caso ci dovesse essere un improvviso bisogno di risorse il sistema ne chiederà in automatico. Se invece il sistema ha disponibile delle risorse scarsamente utilizzate, il sistema ne diminuirà la richiesta. In questo modo si riducono sia i costi sia gli sprechi di risorse (sia per il cliente sia per Microsoft).
I dati e servizi situati nei server Microsoft sono replicati in tre differenti ambienti dello stesso datacenter, selezionabile a piacimento dal cliente. Inoltre, esiste anche il servizio di georeplica che permette di replicare i propri dati e servizi in datacenter diversi.

8.7 Simulazione di risparmio tra locale e cloud

Per questa simulazione è stata presa come riferimento una realtà che conta 30 utenti e viene considerato un periodo di ammortamento delle infrastrutture IT di 5 anni.

8.7.1 Soluzione cloud per 3 server e 1 struttura di backup

Valore investimento per server, licenze e strutture	40.000 €
Costo per singolo esercizio:	
Ammortamento	8.000 €
Costo annuo di gestione (manutenzioni, personale, energia elettrica)	4.000 €
	12.000 €
Soluzione cloud per 30 utenti	**9.000 €**
Differenza	**3.000 €**
Rispamio pari al 25%	

Fonte: infostudi.it

8.7.2 Soluzione Office 365 di Microsoft Exchange

Valore investimento per server, licenze e strutture	9.000 €
Costo per singolo esercizio:	
Ammortamento	1.800 €
Costo annuo di gestione (manutenzioni, personale, energia elettrica)	3.000 €
	4.800 €
Soluzione cloud per 30 utenti	**1.200 €**
Differenza	**3.600 €**
Risparmio pari al 75%	

Fonte: infostudi.it

8.8 Comparazione tra locale e cloud

	On Local	On Cloud
Dati garantiti "georeplicati"	no	si
Business continuity 99,9%	no	si
Monitoraggio HW h24, 7 su 7	no	si
Backup "georeplicati"	no	si
Servizi accessibili ovunque via internet	si	si
Necessità collegamento a internet	no	si

Fonte: infostudi.it

Capitolo 9

Conclusioni

La stesura di questa tesi mi ha permesso di conoscere maggiormente il piano di Disaster Recovery, di farmi capire l'importanza dei dati e di conoscere più a fondo i rischi connessi ai dati aziendali. Studiando i diversi piani di Disaster Recovery aziendali ho compreso meglio la questione delle diverse tipologie e dei livelli di complessità dei piani di Disaster Recovery. Ho notato che le aziende grandi e molto strutturate hanno piani di Disaster Recovery più complessi rispetto ad aziende medio/piccole. Questo si può constatare ad esempio dal personale addetto alla gestione delle emergenze. Infatti, non in tutte le aziende è presente un team appositamente creato per la gestione alla business continuity, nel caso ci fossero problemi che possano interferire sulla continuità della produzione aziendale. La descrizione dei diversi tipi di rischio mi hanno fatto capire quanto sia necessario essere pronti ad ogni disastro (anche remoto) che potrebbe capitare in azienda. Ho inoltre conosciuto diversi standard ISO utili alle aziende. Eseguendo ricerche sugli strumenti cloud ho scoperto differenze dei servizi cloud che prima non conoscevo. Ho compreso meglio l'architettura delle configurazioni RAID che sono molto utilizzate in ambito aziendale. Inoltre, ho capito meglio il Regolamento Europeo 2016/679 e ho percepito meglio la sua applicazione. Ho potuto scoprire le diverse differenze rispetto al codice per la protezione dei dati personali, emanato con il Decreto Legislativo 30 giugno 2003 n. 196. Infine, sono riuscito a comprendere meglio la situazione delle aziende e delle Pubbliche Amministrazioni riguardo l'IT.

Bibliografia

- Snedaker, S 2013, Business Continuity and Disaster Recovery Planning for IT Professionals, Elsevier Science & Technology Books, Rockland, MA. Available from: ProQuest Ebook Central.
- Wallace, M, & Webber, L 2004, Disaster Recovery Handbook, Amacom, New York. Available from: ProQuest Ebook Central.
- LINEE GUIDA PER IL DISASTER RECOVERY DELLE PUBBLICHE AMMINISTRAZIONI ai sensi del comma 3, lettera b) dell'art. 50-bis del DLgs. N. 82/2005 e s.m.i. , DigitPA
- LINEE GUIDA PER IL DISASTER RECOVERY DELLE PUBBLICHE AMMINISTRAZIONI ai sensi del comma 3, lettera b) dell'art. 50-bis del Codice dell'Amministrazione Digitale, Aggiornamento 2013 , AgID
- Piano di Continuità Operativa ICT, Esempio di modello generale, AgID
- REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, Garante per la protezione dei dati personali
- Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019 – 2021, AgID
- Feldheim, D. A. 1984, Computer backup and disaster recovery agreements, Jurimetrics Journal, 24(3), 210-217
- Standard BS ISO 31000:2018

- Standard BS ISO/IEC 27031:2011
- Standard BS ISO/IEC 24762:2008
- https://bologna.repubblica.it/cronaca/2018/04/26/news/bologna_il_sito_del_comune_sotto_attacco_informatico-194878573/
- http://www.aspbasilicata.it/infosalute/alert-virus-riguarda-le-mail-aziendali-le-indicazioni-del-sia
- http://www.ansa.it/sito/notizie/tecnologia/tlc/2019/12/12/170-comuni-nel-mondo-vittime-ransomware_8e77c480-df1d-44cb-860e-d9166e30b255.html
- https://www.gazzettadellevalli.it/valle-camonica/edolo/applicativi-informatici-fermi-nelle-strutture-asst-valcamonica-per-grave-guasto-tecnico-164815/
- https://www.repubblica.it/tecnologia/sicurezza/2017/05/12/news/maxi_attacco_hacker_mondiale_virus_chiede_riscatto_colpita_anche_l_italia_-165285797/
- https://www.agendadigitale.eu/sanita/ransowmare-nella-pa-e-nella-sanita-cosi-prendono-in-ostaggio-i-nostri-dati/
- https://ingv.maps.arcgis.com/apps/webappviewer/index.html?id=2cd378e1029d446a95fbf8d4d33a2669 (I terremoti in Italia del 2019, INGV)
- http://www.treccani.it/vocabolario/uragano/
- https://www.epicentro.iss.it/coronavirus/sars-cov-2
- https://www.bosettiegatti.eu/info/norme/statali/2005_0082.htm
- https://www.gazzettaufficiale.it/eli/id/2016/09/13/16G00192/sg
- https://www.cybersecurity360.it/legal/continuita-operativa-e-disaster-recovery-nelle-pa-nuove-regole-per-creare-un-piano-operativo/
- https://www.agendadigitale.eu/sicurezza/sicurezza-pa-perche-non-e-piu-rimandabile-un-piano-di-disaster-recovery/
- https://www.commissariatodips.it/approfondimenti/phishing/phishing-che-cose/

- https://www.osservatori.net/it_it/osservatori/comunicati-stampa/in-corsa-per-l-italia-digitale
- https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict
- https://blog.osservatori.net/it_it/piano-triennale-ict-pubblica-amministrazione
- https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pubblica_amministrazione_2019_-_2021_allegati20190327.pdf
- https://www.agendadigitale.eu/cittadinanza-digitale/piano-triennale-per-linformatica-nella-pa-il-punto-sullattuazione/
- https://tecnologia.libero.it/cloud-sempre-piu-aziende-guardano-con-favore-alla-nuvola-21159
- https://www.zerounoweb.it/cloud-computing/security-in-cloud-i-5-passi-per-impostare-un-piano-efficace/
- https://www.wired.it/attualita/tech/2018/12/19/ora-cloud/?refresh_ce=
- www.datamanager.it/2018/10/cresce-ladozione-del-cloud-da-parte-delle-imprese-italiane/
- http://www.infostudi.it/office365-introduzione/itemlist/category/category/91
- http://www.infostudi.it/lavorare-in-cloud-i-benefici-del-cloud
- www.infostudi.it/microsoft-azure-il-nuovo-ambiente-cloud-di-microsoft/
- http://www.infostudi.it/lavorare-in-cloud-il-risparmio-per-la-tua-azienda/
- https://www.iusinitinere.it/la-sicurezza-del-trattamento-analisi-dellarticolo-32-gdpr-16205
- https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679&from=IT
- https://robertarapicavoli.it/gdpr-quali-misure-sicurezza-adottare/

- http://www.privacy-regulation.eu/it/32.htm
- http://www.privacy-regulation.eu/it/33.htm
- http://www.privacy-regulation.eu/it/r74.htm
- http://www.privacy-regulation.eu/it/r75.htm
- http://www.privacy-regulation.eu/it/r83.htm
- https://www.nakivo.com/blog/backup-types-explained-full-incremental-differential-synthetic-and-forever-incremental/
- https://www.recovery-data.it/differenti-tipologie-di-backup/
- https://www.01net.it/differenze-fra-i-vari-tipi-di-backup/
- https://www.iperiusbackup.net/tipi-di-backup-di-iperius-completo-incrementale-differenziale/
- https://www.cwi.it/cloud-computing/differenza-iaas-paas-e-saas-110488
- https://www.opencloudict.it/cosa-significa-iaas-saas-daas/
- https://www.aruba.it/magazine/cloud/iaas-paas-saas-cloud-a-confronto.aspx
- https://www.informaticapertutti.com/raid-che-cose-come-funziona-e-come-si-usa/
- https://it.wikipedia.org/wiki/RAID
- https://www.crowd-funding.cloud/it/crowdfunding-il-finanziamento-della-folla-o-dei-folli-187.asp
- https://www.crowd-funding.cloud/it/definizione-139.asp
- https://mamacrowd.com/article/tipi-di-crowdfunding
- https://www.settesere.it/it/notizie-romagna-faenza-mirko-guerra-amministratore-delegato-della-bitways-anoi-come-la-fenicea-n21416.php
- https://www.ilbuonsenso.net/bitways-faenza/

- https://bitways.it/idea-ginger/
- https://www.ideaginger.it/progetti/dall-esperienza-del-disastro-al-miglioramento-della-disaster-recovery.html
- https://bitways.it/2019/11/06/rinascere-dalle-ceneri/
- https://bitways.it/2019/12/11/il-successo-del-progetto-crowdfunding-e-i-prossimi-passi/
- https://blogs.technet.microsoft.com/mspfe/2012/03/08/a-microsoft-word-document-template-for-disaster-recovery-planning/
- www.netjapan.com
- searchdisasterrecovery.techtarget.com
- https://www.pamercato.it/wp-content/uploads/2018/06/Piano-BC-e-DR_rev01.pdf
- https://www.scuolecertosa.edu.it/attachments/article/43/Disaster%20Recovery.pdf
- https://www.consorziosea.it/wp-content/uploads/Piano-di-Continuit%C3%A0-Operativa-e-di-Disaster-Recovery.pdf
- https://www.cpiareggionord.edu.it/attachments/article/188/Linee_Guida_per_il_disaster_recovery_delle_PA.pdf
- https://www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/modello-pco-per-pa_0.pdf
- https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/linee-guida-dr.pdf
- http://www.continuitycentral.com/feature0660.html
- https://www.unocloudbackup.it/differenza-tra-disaster-recovery-plan-e-business-continuity-plan/
- https://searchdisasterrecovery.techtarget.com/tip/Seven-business-continuity-strategy-planning-mistakes

- https://www.aruba.it/comunicatistampa/pdf/Articolo%20d%27opinione,%20come%20realizzare%20un%20buon%20piano%20di%20Disaster%20Recovery.pdf
- https://www.01net.it/la-checklist-per-un-piano-di-disaster-recovery/
- www.qualitiamo.com/risk%20management/risk%20management.html